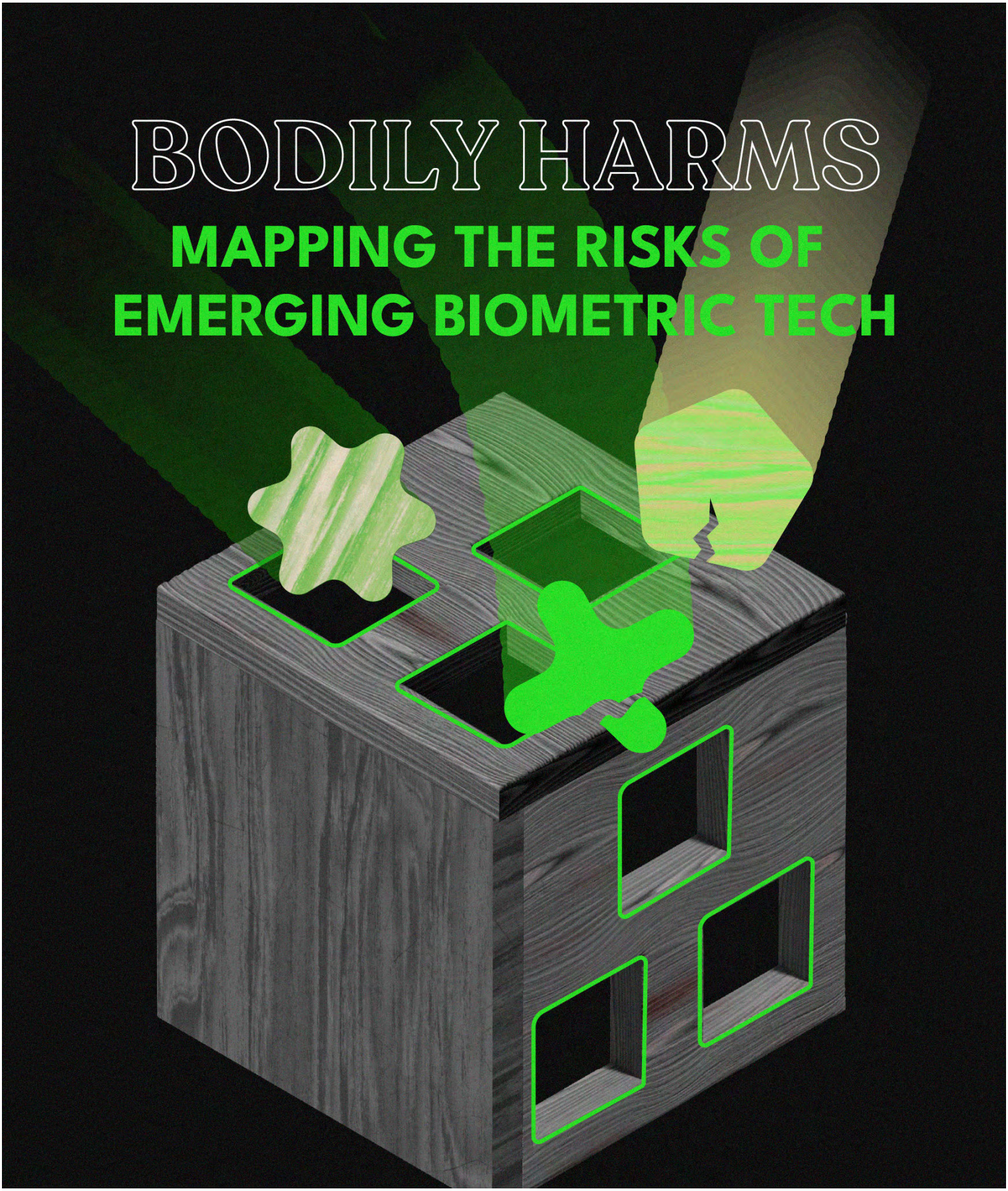
BODILY HARMS

MAPPING THE RISKS OF EMERGING BIOMETRIC TECH



accessnow

Access Now (accessnow.org) defends and extends the digital rights of people and communitiesat risk. As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

Acknowledgements

This paper is an Access Now publication, written by Xiaowei Wang from UCLA's Center on Race and Digital Justice/ELISAVA School of Design and Engineering and Shazeda Ahmed from UCLA's Center on Race and Digital Justice, with additional contributions from Daniel Leufer from Access Now.

The authors would like to thank the Access Now team members who provided support, including Méabh Maguire, Loren Giordano, Sage Cheng, Gaspar Pisanu, Giulio Coppi, Marianne Díaz Hernandez, and Willmary Escoto. We appreciate the help of all the interviewees, researchers, and experts who provided us with key insights and information for this publication, and additionally Dr. Crystal Lee from MIT.

For more information, please visit:
https://www.accessnow.org

Contact:
Daniel Leufer | Senior Policy Analyst and Emerging Technologies Policy Lead
daniel.leufer@accessnow.org

Published in October 2023

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In the following report, we draw on document analysis and expert interviews to explain how an understanding of the political economy of biometric systems can inform future paths to their governance. Through a two-by-two matrix of "hard biometrics" versus "soft biometrics," and what we loosely characterize as "low-tech" versus "high-tech," we provide examples of different biometric data collection types and use cases to demonstrate how the companies that produce these technologies have continuously thwarted attempts at regulation. Across analyses of voice biomarkers, voice recognition, eye tracking, and neurotech, we highlight the following findings and themes:

- We sort the biometric technologies described in this report into a two-by-two matrix to map "hard" and "soft" biometrics that we characterize as "high-tech" and "low-tech." "Hard" biometrics signify biometric systems used exclusively for identification or verification (e.g., identification for access to government-issued resources), while "soft" biometrics are used to classify people or infer attributes such as age, gender, or emotional state. "Low-tech" refers to systems such as video cameras, while "high-tech" refers to more complex systems, such as implantable neurotech that requires an expert to insert it into the body.

- Many of the current and proposed uses of the biometric technologies described in this report are not novel, and have already been seen in the use of so-called "emotion recognition" technologies that rely on computer vision to categorize people's emotions. From monitoring and assessment of behavior and performance in schools, cars, workplaces, and public spaces such as airports, to psychometric and diagnostic uses, commercial applications of the biometric technologies in all four quadrants of our matrix are growing by the day.

- Biometric technologies across the matrix are used to create baselines of what constitute "normal" behaviors and bodies, which further reinforces unequal treatment of people whose bodies and behaviors do not adhere to this normative frame. Combined with the exclusion of disabled people from the process of deciding whether and how to build these technologies, or extremely late-stage consultation with affected communities, this ensures that biometric systems perpetuate ableism, inequality, and other harms.

- Biometric tech producers have established a prevailing narrative that such technologies are inherently "good" for society, particularly if they can "cure" specific health conditions or disabilities. Rather than subscribing to such ableist ideas of curative violence, it is essential to examine biometric technologies and their purported good from a disability justice framework, which centers disabled people as active designers of technologies, rather than as mere users after the fact.

- Biometric technologies are particularly prone to "function creep," or the repurposing of a technology's initial, bounded use into another, often more harmful application. For example, a biometric voice system that purports to detect mental distress or anxiety markers, or an eye-tracking tool that tracks attention and "nervousness" for use in a clinical setting can then be repurposed in "AI lie detectors" used by law enforcement and the military.

- When we spoke with experts about privacy concerns around the use of voice biomarkers and neurotech, they were enthusiastic about the potential for privacy-preserving machine learning techniques such as federated learning to protect patients and clinical trial subjects' data. However, federated learning requires coordinated compliance across a wide range of actors, which can be difficult to establish. In focusing on federated learning as a technical solution, many technology developers also fail to address that some use cases are undesirable and harmful, even if they preserve privacy.

AN INTRODUCTION TO BIOMETRICS

In recent years, biometric systems have proliferated around the world, whether used in identification for accessing state-provided welfare benefits or to allegedly classify socially understood forms of emotion.[1] The rise of such biometric identification systems and their derivative uses has paralleled the rise of artificial intelligence (AI). With the proliferation of cheaper hardware, sensors, processing capabilities, and cloud infrastructure, the uses of biometric systems have increased globally and grown more common in different contexts – whether at national borders, to access state benefits, or in our own homes.[2]

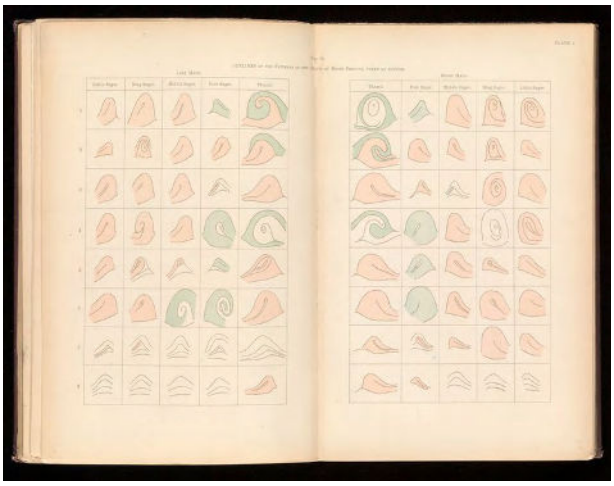


Photo: Wellcome Collection

In the late 1800s, Francis Galton, one of the founders of eugenics, developed a method of systematically identifying and comparing fingerprints, which gave rise to a precursor of biometrics that spread throughout many colonial governments and bears similarities to its modern day form.[3] Biometrics has evolved as a technical discipline and claims that make major leaps, such as the capacity for "profiling humans from their voice,"[4] have given rise to an industry subject to a larger political economy, regulation, and the financial impacts of a tech-driven innovation economy.[5]

1 Marda, Vidushi and Ahmed, Shazeda. Emotional Entanglements: China's Emotion Recognition Market and Its Implications for Human Rights, (Jan 25, 2021). ARTICLE 19 report. https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf.

2 Australian Border Force, "SmartGates." https://www.abf.gov.au, https://www.abf.gov.au/entering-and-leaving-australia/smartgates. See also Ratcliffe, Rebecca. "How a Glitch in India's Biometric Welfare System Can Be Lethal." The Guardian, (Oct 16, 2019). https://www.theguardian.com/technology/2019/oct/16/glitch-india-biometric-welfare-system-starvation. Jillson, Elisa. "Hey, Alexa! What Are You Doing with My Data?" Federal Trade Commission, (Jun 13, 2023). https://www.ftc.gov/business-guidance/blog/2023/06/hey-alexa-what-are-you-doing-my-data.

3 Migozzi, Julien. "Apartheid by Algorithm." Logic(S) Magazine, (August 2022). https://logicmag.io/home/apartheid-by-algorithm/.

4 The phrase "profiling humans from their voice" comes from Rita Singh's book of the same title.

5 Breckenridge, Keith. Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present. Cambridge, Cambridge University Press, 2016.

For the purposes of our report, we examine biometrics across a two-by-two matrix spanning "hard" and "soft" biometrics along one axis, and what we refer to as "low-tech" and "high-tech" along the other. While biometrics has generally been defined as "automated methods of recognizing and verifying the identity of individuals based on physiological or behavioral attributes," they can also be divided into the designations of "hard" versus "soft" biometrics.[6] Hard biometrics are seen as the identification of individuals based on physiological and behavioral attributes, as well as the claims of deducing "other types of attributes of an individual from the same data (...) such as age, gender, ethnicity, height."[7]

Biometric data is usually considered "hard" if it meets each of these four basic requirements: it can be measured (collectability); it relates to a characteristic that all people have (universality); it relates to a characteristic that is distinctive in every person (uniqueness); and it relates to a permanent attribute (permanence). By contrast, soft biometrics include "behavioral attributes" or attributes that are generalizable rather than specific to an individual — for example, the condition of being depressed, anxious, or other clinical and emotional conditions.

As the use of biometric data collection combined with AI systems has increased in many contexts, so has pushback from civil society and activists, particularly those working in privacy, data protection, and digital rights.[8] In the European Union (E.U.), the General Data Protection Regulation (GDPR) prohibits the processing of "special categories of personal data," including biometric data for the purposes of identification, as well as "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership."[9] However, this prohibition is subject to wide exceptions for investigating crimes and maintaining "public security," and digital rights activists are pushing for increased protections in the proposed E.U. AI Act.[10] While the original draft of the AI Act proposes some limited restrictions, various stakeholders,[11] including E.U. data protection authorities and certain political groups[12] are calling for full bans on "remote biometric

6 Schiering, Ina et al. Privacy and Identity Management: Between Data Protection and Security : 16th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Privacy and Identity 2021, Virtual Event, (Aug 16-20, 2021). Revised Selected Papers. Vol. 644. Springer, 2022. Print.

7 Dantcheva, Antitza, Petros Elia, and Arun Ross. "What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics." IEEE Transactions on Information Forensics and Security 11, no. 3 (March 2016): 441–67. https://doi.org/10.1109/TIFS.2015.2480381.

8 Campaigns and letters include: Ban Biometric Surveillance. Access Now. https://www.accessnow.org/campaign/ban-biometric-surveillance/; Reclaim Your Face. https://reclaimyourface.eu/; and Tire Meu Rosto Da Sua Mira (Open Letter to Ban the Use of Digital Facial Recognition Technologies in Public Security). https://tiremeurostodasuamira.org.br/en/open-letter/.

9 Article 9, GDPR states that "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited." This is followed by a broad list of exceptions in Article 9(2). https://eur-lex.europa.eu/eli/reg/2016/679/oj.

10 European Digital Rights, Remote biometric identification: a technical & legal guide, (Jan 23, 2023). https://edri.org/our-work/remote-biometric-identification-a-technical-legal-guide/.

11 EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), (Jun 18, 2021). https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf.

12 Fighting for a Ban on Biometric Mass Surveillance in Public Spaces. The Greens/EFA in the European Parliament. https://www.greens-efa.eu/en/campaigns/ban-biometric-mass-surveillance.

identification," as well as emotion recognition and discriminatory forms of biometric categorisation.[13]

Alongside the growth of regulatory frameworks, there is also pushback from government and industry on the need to balance regulation with "innovation" and industry growth. In the wake of a global pandemic, the use of biometric technologies in the medical field (particularly for telemedicine, remote diagnosis and treatment, quarantine, and border security) or "contactless" biometric technologies for ID and payment are often used as arguments for beneficial development of biometric technologies, and against their regulation.

Our mapping of the biometric tech matrix demonstrates that it is not the fulfillment of security benefits or other promises of veracity or functionality that keep biometric systems in circulation. Rather, state and market forces centering narratives of security and optimization incentivize the development of biometrics.

For example, biometric identification systems are implemented by governments in state-supported welfare for the intended purposes of countering purported welfare fraud and optimizing the delivery of benefits, despite many studies demonstrating that true "welfare fraud" is rare and, more often than not, a socially constructed moral panic.[14] Another example of how securitization narratives create a market for biometrics is seen in their use at national borders, allegedly to combat "security risks," such as post-9/11 U.S. terrorism. Hefty government contracts have been awarded to such companies, yet deeper analysis calls into question how effective such systems are at providing more "safety," rather than simply performing what some experts term "security theater."

In both examples, the manufactured crisis of "welfare fraud" and the normalization of "security theater" creates a landscape of private tech companies competing for government contracts, particularly private tech companies receiving investment and grants from governments and government-adjacent venture capital firms. The resulting upswell in research, development, and investment is often seen by governments as a net positive for the economy.[15] It is this global political economy — a web of companies, state agencies, and lax regulation or policies — that underpins the creation and

13 See the following issue papers (all May 2022):
Prohibit all Remote Biometric Identification (RBI) in publicly accessible spaces, https://edri.org/wp-content/uploads/2022/05/Prohibit-RBI-in-publicly-accessible-spaces-Civil-Society-Amendments-AI-Act-FINAL.pdf;
Prohibit discriminatory biometric categorisation in the AI Act, https://www.accessnow.org/wp-content/uploads/2022/05/Amendments-to-the-AI-Acts-treatment-of-biometric-categorisation.pdf;
Prohibit emotion recognition in the Artificial Intelligence Act, https://www.accessnow.org/wp-content/uploads/2022/05/Prohibit-emotion-recognition-in-the-Artificial-Intelligence-Act.pdf.

14 See Chunn, D. E., & Gavigan, S. A. M. (2004). Welfare Law, Welfare Fraud, and the Moral Regulation of the 'Never Deserving' Poor. Social & Legal Studies, 13(2), 219–243., Devereux, Eoin, and Martin J. Power. "Fake News? A Critical Analysis of the 'Welfare Cheats, Cheat Us All' Campaign in Ireland." Critical discourse studies 16.3 (2019): 347–362., Gustafson, Kaaryn S.. Cheating Welfare: Public Assistance and the Criminalization of Poverty, New York, USA: New York University Press, (2011), and Yoo, Grace J. (2008) Immigrants and Welfare: Policy Constructions of Deservingness, Journal of Immigrant & Refugee Studies, 6:4, 490-507, DOI: 10.1080/15362940802479920.Mosher, Janet, and Joan Brockman. Constructing Crime. UBC Press, (May 10, 2010).

15 See Amoore, Louise. "Biometric borders: Governing mobilities in the war on terror." Political geography 25.3 (2006): 336-351, Ackerman, Spencer. "Insider: $56 Billion Later, Airport Security Is Junk." WIRED, (Dec 6, 2011). https://www.wired.com/2011/12/unsafe-skies/, Schneier, Bruce. Beyond Fear: Thinking Sensibly about Security in an Uncertain World. New York, Springer Science+Business Media, (2013), and O'Neil, Patrick H. "Complexity and Counterterrorism: Thinking About Biometrics." Studies in conflict and terrorism 28.6 (2005): 547–566.

proliferation of biometric technologies, and it is this which presents the greatest challenge to civil society pushback.

As "hard biometrics," and the use of biometrics to verify people's legal identity, become increasingly regulated, we are seeing the parallel rise of soft biometrics used in a gray zone: technologies purporting to categorize emotional states, infer complex personality traits, or diagnose mental illness and medical conditions such as Parkinson's disease or autism.[16] This report intertwines a critical look at the political economy and context of biometric technologies' production with a framework that echoes much of the work being done in disability justice, distinct from disability rights.[17]

In a disability justice framework, the social model of disability reveals the ways disability intersects with a number of overlapping, marginalized positions.[18] It also shows how disability is socially constructed; it is not an individual medical problem that needs to be "solved" or "fixed." Additionally, the framework of disability justice allows us to understand the historical and ongoing ways that designations of mental illness carry uneven consequences for marginalized communities depending on race, gender, class, caste, and immigration status. This is a particularly relevant point given how the emerging shift toward soft biometrics often purports to solve the rising tide of mental illness in a post-pandemic world.[19]

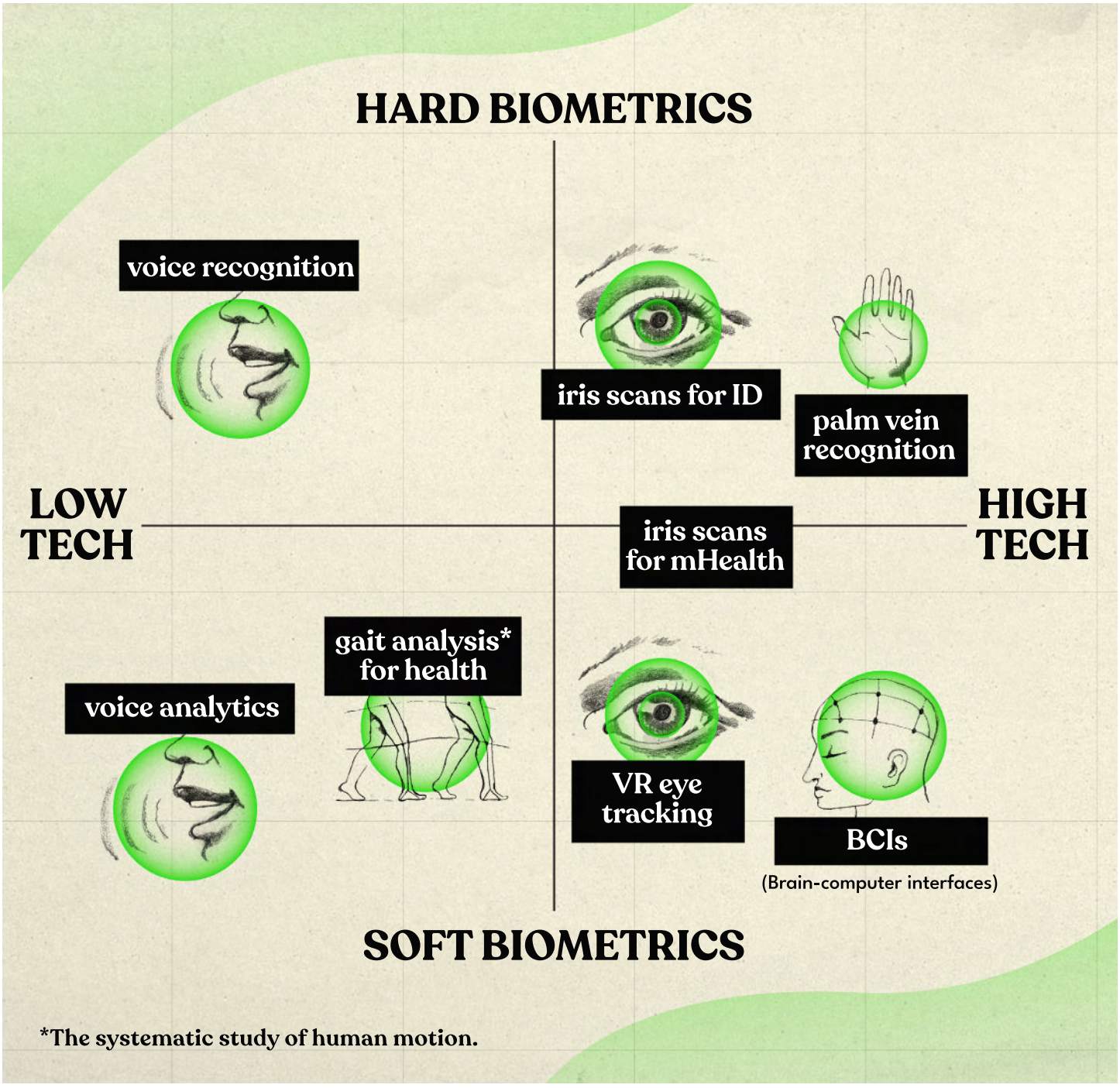
16 Os Keyes, Automating autism: Disability, discourse, and Artificial Intelligence, (May 2020). https://digitalcommons.odu.edu/cgi/viewcontent.cgi?article=1021&context=sociotechnicalcritique.

17 CODE Associated Students Commission on Disability Equity "What Is Disability Justice? | CODE." https://code.as.ucsb.edu/, (2020). https://code.as.ucsb.edu/what-is-disability-justice/.

18 Bailey, Moya, and Izetta Autumn Mobley. "Work in the Intersections: A Black Feminist Disability Framework." Gender & Society 33, no. 1 (Feb 1, 2019): 19–40. https://doi.org/10.1177/0891243218801523.

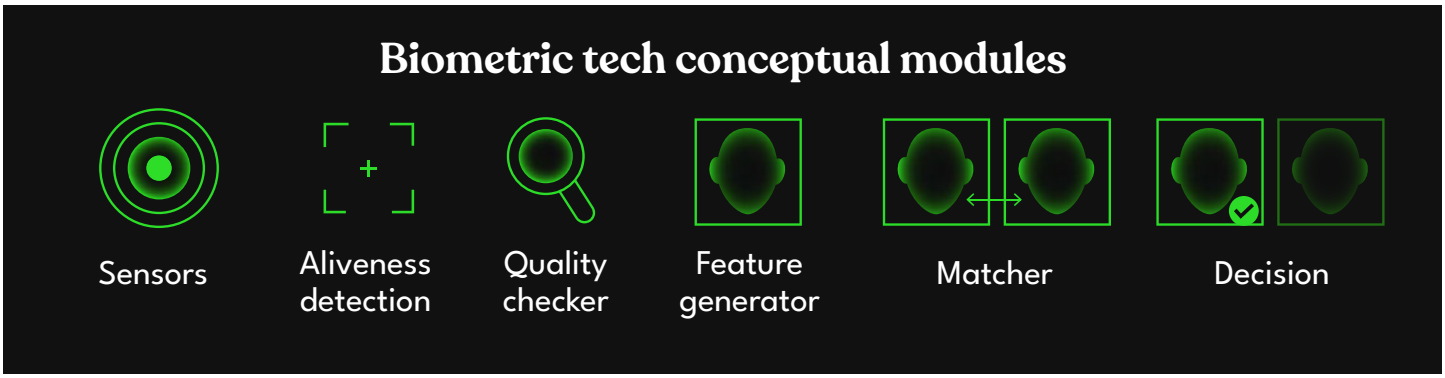
19 Nirmita Panchal, Heather Saunders, Robin Rudowitz, and Cynthia Cox. The Implications of COVID-19 for Mental Health and Substance Use. KFF, (Mar 20, 2023). https://www.kff.org/coronavirus-covid-19/issue-brief/the-implications-of-covid-19-for-mental-health-and-substance-use/.

WHAT'S IN THE BIOMETRIC TECH MATRIX?



The term "biometrics" has typically referred to biometric systems used to verify or determine the identity of an individual based on physical or physiological characteristics (i.e., fingerprints, iris or gait recognition).[20] However, biometric data and biometric systems are increasingly used to profile, categorize, and classify people without "identifying" them in the narrow sense of confirming their personal identity.

20 See supra note 7.



Biometric technologies typically contain six conceptual 'modules' that include hardware (such as the sensors) and algorithms (such as aliveness detection): "sensors, aliveness detection, quality checker, feature-generator, matcher, and decision modules."[21] In this report, we generalize each biometric technology we investigate into two parts: 1) biometric data that is captured via sensors, and 2) the biometric system itself.

During the biometric data capture process, sensors can capture physiological measurements such as palm vein imagery, voice data, or iris scans. These measurements are converted into data that are then input into biometric systems. Biometric systems include a range of algorithms that process and make the captured biometric data useful. On the simpler end, these algorithms can extract a biometric template from an image of a person's fingerprint and match it against others in a database in order to identify the person.[22] They can also be more complex, using AI — in particular mathematical models — to surface "biomarkers," or patterns within physiological or behavioral data.

The wide-ranging nature of these systems means that each component of a biometric system is often siloed within research and industry organizations. One company might make the sensor or biometric capture device. Another company might make the matching algorithm and sell it packaged as an API (application programming interface) or SDK (software development kit). Other companies offer full systems, including the capture device and proprietary software to classify and process biometric data.

Breaking down a biometric system into components helps us understand the complex supply chains and interdependencies at play in these systems, which create gaps in oversight and complicate efforts to hold actors within the production chain responsible for harms. At the same time, it also ensures the continuous creation of these technologies. For example, an increase in use of biometric algorithms raises demand in the hardware industry that specializes in sensors and biometric data capture.

It is important to highlight the difference between biometric data and a biometric system in order to understand the slippages between the data itself, and the claims that companies and researchers make around the veracity of biometric systems, particularly

21 ISO/IEC 2382-37:2021. "Information technology -- Vocabulary -- Part 37: Biometrics." International Organization for Standardization. https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en:term:3.1.1.
22 Ratha, Nalini K., Andrew Senior, and Ruud M. Bolle. "Automated Biometrics." In Advances in Pattern Recognition — ICAPR 2001, edited by Sameer Singh, Nabeel Murshed, and Walter Kropatsch, 447–55. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2001. https://doi.org/10.1007/3-540-44732-6_46.

regarding these systems' underlying classification algorithms. An algorithm built to identify or classify people based on their biometric data, through matching or categorization, is the result of research and beliefs about reproducibility of the research's results. The data itself is ultimately, simply data. Any claim that an algorithm can detect or classify behavior based on biometric data cannot be taken as a numerical or mathematical claim; it is a claim around interpretability. As a process of interpreting and modeling data, biometric algorithms must be subject to the same level of scrutiny as any sort of scientific research, which is often a rigorous peer-reviewed process.

Unfortunately, it is difficult to prove if private companies uphold this level of peer review and scrutiny, as they claim their technologies are proprietary. Moreover, peer review of computer science papers has often over-emphasized technical errors at the expense of concerns around social issues underlying the research. For instance, after a paper claiming researchers could infer criminality from individuals' facial features was published, over 1,000 academic researchers petitioned the journal to remove the article.[23]

Throughout this report, we use the notion of a biometric "tech matrix," with one axis highlighting areas where the sensor or capture device increases in complexity. For example, on the "low-tech" end of the matrix, video cameras and voice recorders can capture biometric data. Technologies on the low-tech end of the spectrum tend to be more widely commercially available and thus used more often. On the "high-tech" end, more specialized equipment used to capture brain wave data or read and write to the brain is, for now, typically only available within labs or other highly controlled settings. On the other axis of this matrix, we use the terms "hard" and "soft" biometrics to draw attention to tendencies in how low- and high-tech biometric systems are put to use. "Hard" biometrics roughly denotes instances where the biometric system's intended use is solely identification or recognition, typically in order to access state services such as welfare benefits. By contrast, "soft" biometrics are increasingly common within medical uses, as well as for AI "polygraphs" that claim to detect whether someone is lying or not. Such cases include the proposed EU's short-lived iBorderCtrl lie detection system or technologies being used in law enforcement and courtroom settings such as polygraphs tracking eye movement.[24]

23 Fussell. S, "An Algorithm That "Predicts" Criminality Based on a Face Sparks a Furor," WIRED, (Jun 24, 2020). https://www.wired.com/story/algorithm-predicts-criminality-based-face-sparks-furor/.

24 van der Ploeg, I. (2011). Normative Assumptions in Biometrics: On Bodily Differences and Automated Classifications. In: van der Hof, S., Groothuis, M. (eds) Innovating Government. Information Technology and Law Series, vol 20. T.M.C. Asser Press. https://doi.org/10.1007/978-90-6704-731-9_3; Virginio Cantoni, Mirto Musci, Nahumi Nugrahaningsih, Marco Porta. Gaze-based biometrics: An introduction to forensic applications. Pattern Recognition Letters, Volume 113, (2018). Pages 54-57. https://doi.org/10.1016/j.patrec.2016.12.006; Ryan Gallagher and Ludovica Jona. "We Tested Europe's New Lie Detector for Travelers — and Immediately Triggered a False Positive." The Intercept. (Jul 26, 2019). https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/. Zeitchik, Steven "A Utah Company says its revolutionized truth-telling technology. Experts are skeptical," Washington Post, (Nov 15, 2021). https://www.washingtonpost.com/technology/2021/11/15/lie-detector-eye-movements-converus/.

HOW ARE THESE BIOMETRIC TECHNOLOGIES BEING USED?

Beyond identification and recognition systems, AI-driven biometric systems are increasingly used throughout the world to register and purportedly identify affect, or emotions and moods.[25] These systems are marketed as being able to recognize emotions such as anger or happiness[26] and, in some cases, to increase the "efficiency" of medical diagnoses for conditions ranging from autism to neurodegenerative and cardiovascular disorders.[27] As industry and academic research pours greater resources into deploying these "soft" biometric systems, we recognize a broader trend in both domains: technical development and research of AI-driven biometric classification and diagnosis systems stemming from perceived benevolent motivations, particularly around curing and diagnosing disease.

Some technical researchers, including some of the experts we spoke to, repeatedly frame such novel technologies as potentially risky and causing harm to vulnerable populations, raising unresolved questions around consent and lack of representation and inclusion from vulnerable populations. Yet they also voiced beliefs that the benefits outweigh the risks. AI-driven biometric systems generally rely on large amounts of training data collected from subjects, labeled, and then fed into mathematical models that "learn" from the training data. For instance, thousands of audio clips of voice recording data can be individually labeled as "depressed" or "not depressed," and fed into a mathematical model to be "trained." Theoretically, the model can then label any new voice clip it is given with the likelihood of the speaker being "depressed" or "not depressed." It is worth noting that the training data required to create such models is often obtained without

25 Stark and Hoey note the long-standing debate on difference between "emotion" and "affect," describing emotion as "a compound phenomenon variously consisting of evaluative, physiological, phenomenological, expressive behavioral, and mental components," and drawing on theorist Deborah Gould's definition of affect as "nonconscious and unnamed, but nonetheless registered, experiences of bodily energy and intensity that arise in response to stimuli." Luke Stark and Jesse Hoey. (2021). The Ethics of Emotion in Artificial Intelligence Systems. In Proceedings of ACM Conference on Fairness, Accountability, and Transparency (FAccT'21). ACM, New York, NY, USA. pp 782-783. https://doi.org/10.1145/3442188.3445939.

26 Marda, Vidushi and Ahmed, Shazeda. Emotional Entanglements: China's Emotion Recognition Market and Its Implications for Human Rights. ARTICLE 19, (Jan 25, 2021). https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf.

27 Vargas-Cuentas, Natalia I., Avid Roman-Gonzalez, Robert H. Gilman, Franklin Barrientos, James Ting, Daniela Hidalgo, Kelly Jensen, and Mirko Zimic. "Developing an Eye-Tracking Algorithm as a Potential Tool for Early Diagnosis of Autism Spectrum Disorder in Children." PLOS ONE 12, no. 11 (Nov 30, 2017): e0188826. https://doi.org/10.1371/journal.pone.0188826., Fagherazzi, Guy et al. "Voice for Health: The Use of Vocal Biomarkers from Research to Clinical Practice." Digital Biomarkers 5.1 (2021): 78–88. Web.

explicit consent, whether from video platforms like YouTube or, for image-based biometric prediction models, from sources like visa applications.[28]

These seemingly benevolent technologies are not only subject to lax regulation around the use of biometrics and AI in mobile health contexts,[29] but also to "function creep," where technology (and in particular, mathematical models) developed for one specific purpose become monetized and deployed across other contexts.[30] For example, a biometric voice system that purports to detect mental distress or anxiety markers, or an eye-tracking tool that tracks attention and "nervousness" for use in a clinical setting can then be then repurposed for "AI lie detectors" used in law enforcement and military contexts.[31]

As we learned from speaking with researchers, ethicists, and industry experts, there are very real functionality limitations and genuine concerns around the reproducibility of such technologies' results. Not only do they often rely on imprecise science and experiments whose results cannot be consistently reproduced, but they also exacerbate and exaggerate existing social inequities, rather than delivering on nebulous claims of alleviating such issues. Additionally, the nature of biometric data capture and storage can often infringe on existing privacy laws and consent, e.g., voice capture in the field can result in collecting background voices from people who have not consented to being recorded.

We heard from our expert interviewees about their concerns around the use of biometric technologies to striate social groups or deepen inequity, particularly when these technologies help gatekeep state benefits during fiscal austerity or further criminalize marginalized populations already subject to state abandonment. Given the growing use of many "soft" biometric technologies in law enforcement, we also point to the very shaky, often redrawn line between what is considered "criminal" or not, and how the only consistent output of such technologies is the reproduction of existing biases around who is inherently criminalized.

28 See Keyes, Os; Nikki Stevens, and Wernimont Jacqueline, "The Government Is Using the Most Vulnerable People to Test Facial Recognition Software," Slate, (Mar 17, 2023). https://slate.com/technology/2019/03/facial-recognition-nist-verification-testing-data-sets-children-immigrants-consent.html, and Keyes, Os, and Jeanie Austin. "Feeling Fixes: Mess and Emotion in Algorithmic Audits." Big data & society 9.2 (2022): 205395172211137–. Web.

29 Nurgalieva, Leysan, David O'Callaghan, and Gavin Doherty. "Security and Privacy of MHealth Applications: A Scoping Review." IEEE Access 8 (2020): 104247–68. https://doi.org/10.1109/ACCESS.2020.2999934.

30 Mordini, E., & Massari, S. (2008). Body, biometrics and identity. Bioethics, 22(9), 488–498. https://doi.org/10.1111/j.1467-8519.2008.00700.

31 Boguslaw, Daniel. "Lie Detector Firm Lobbies CIA, DOD on Automated Eye-Scanning Tech." The Intercept. (Apr 7, 2023). https://theintercept.com/2023/04/07/lie-detector-dod-cia-converus/; Murphy, Brett. "They Called 911 for Help. Police and Prosecutors Used a New Junk Science to Decide They Were Liars." ProPublica, (Dec 28, 2022). https://www.propublica.org/article/911-call-analysis-fbi-police-courts; Voice Stress Analyzer. SecIntel. https://www.secintel.com/ecom-prodshow/voice_stress_analyzer.html.

WHY BIOMETRIC TECH IS ABLEIST

In the context of biometric technologies and their regulation, it is important to have a framework that accommodates the complex lived realities of people encountering these technologies on the ground. In the process of researching this report and through interviews with experts, while we found a general agreement that biometric surveillance should be regulated in some way, an overarching theme we heard from some interviewees was an insistence that biometric technologies that purport to diagnose or classify emotion and affect should be regulated in a more lax manner, given their potential for helping people with illness, disability and other clinical or therapeutic uses. While the degree of regulation is debated by experts, academics, and industry researchers, there are broader claims from some research scientists that regulation would infringe upon the rights of disabled to people to access these technologies; an argument that has been framed around negative and positive rights.[32]

This report seeks to foreground disability and the claims of biometric technologies to diagnose and cure in critical terms. The term "disability justice" was coined by activists Patty Berne, Mia Mingus, and Stacey Milbern.[33] As a framework, it builds upon the disability rights movement, advocating for disabled people in the context of the social model of disability, as well as the interlocking systems of oppression that disabled people face. The social model of disability is counter to the medical model (a form of viewing disability through an individual, medicalized lens that needs to be solved or cured for), and understands how society constructs disability as a condition.

For example, if someone in a wheelchair cannot get to the door because there are only stairs, the medical model of disability sees the issue as being that this person is disabled and needs prosthetics. The medical model of disability gives rise to what Liz Jackson, Alex Haagaard, Rua Williams, and others term a "disability dongle," a seemingly innovative solution or object created by designers and engineers despite concerns from disabled persons.[34] On the other hand, the social model of disability sees the issue as being that society has not created alternative forms of access for the person using a wheelchair, such as a ramp.[35]

Disability justice builds upon disability rights work on creating forms of access. Disability justice activists also advocate for understanding the complex, intersectional, and diverse experiences of disability based on race, gender, class, and immigration status. At the heart of disability justice is a focus on countering ableism, as well as recognizing that experiences of disability are not a monolith.

32 "Neuroethics: An Ethics of Technology, with Dr. Joseph Fins." Accessed (May 25, 2023). https://www.carnegiecouncil.org/media/series/aiei/neuroethics-ethics-technology-joseph-fins.

33 For an overview definition of disability justice, see Associated Students Commission on Disability Equity https://code.as.ucsb.edu/what-is-disability-justice/, which draws upon Berne, Patty, "Disability Justice — a working draft", Sins Invalids, (Jun 10, 2015). https://www.sinsinvalid.org/blog/disability-justice-a-working-draft-by-patty-berne.

34 Jackson, Liz, Haagaard, Alex and Williams, Rua. Disability Dongle. Platypus, (Apr 19, 2022). https://blog.castac.org/2022/04/disability-dongle/.

35 Bailey, Moya, and Izetta Autumn Mobley. "Work in the Intersections: A Black Feminist Disability Framework." Gender & Society 33, no. 1 (Feb 1, 2019): 19–40. https://doi.org/10.1177/0891243218801523.

In talking to disability justice advocates, as well as advocacy groups representing those whose medical and mental health conditions such technologies ostensibly "help," we were introduced to the concept of "curative violence," a key tactic of ableism. Curative violence describes an ethics of cure where "curing" a disability or disease is seen as so innately desirable that the subject is destroyed through the curative process.[36] The concept reveals how many of the ethics systems deeply embedded within biometric technologies research and development are "normative ethics," relying on statistical definitions of what is "normal" versus what is "deviant."[37] In turn, they often tie disability to justifications for perpetuating inequity along gender, race, and sexual orientation lines.[38]

Disability justice recognizes how ableism intersects with other systems such as racism and sexism. Vanessa Thompson's research on racialised groups in the E.U., for example, examines how "racialized people who identify or are categorized as mad, neurodiverse, mentally ill, psychiatric survivors, and disabled are particularly vulnerable to police harassment and violence."[39] Ableism affects everyone, and is tied into assumptions of who is considered "deserving" of state benefits. For example, the complex, fraught relationship that transgender communities face as part of biometric identity verification in India's Aadhaar system, which governs access to state benefits, means complying with dominant, inherently discriminatory state conceptions of gender and physiology.[40]

Such normative ethics rely on notions of individual privacy and of consent (e.g., end-user licensing agreements, written consent) as regulatory mechanisms, rather than on more expansive frameworks that protect vulnerable populations and over-surveilled marginalized groups who have a steep power differential with the state, such as migrants. Additionally, adhering to such normative ethics casts vulnerable groups, such as disabled persons and migrants, as subjects of biometric research and innovation, rather than as researchers and active participants in the process. This barrier to treating vulnerable groups as co-designers of the technology further impedes opposition to the argument that the "positive potential" of emergent biometric technologies potentially outweighs their harms.

As we unpack in this report's specific case studies, these harms cannot be addressed without centering marginalized communities, such as the disabled community, throughout the building of these technologies. The currently dominant approach of consulting with these communities at the last minute as research subjects or end users is untenable, and will only continue to reproduce harm regardless of other types of regulatory interventions. In addition to expanding ideas of consent and rethinking privacy, we will

36 Kim, Eunjung. Curative Violence : Rehabilitating Disability, Gender, and Sexuality in Modern Korea. Durham: Duke University Press, (2016). Web. 37 Moura, I. (2023). https://read.dukeupress.edu/books/book/9/Curative-ViolenceRehabilitating-Disability-Gender.
37 Moura, I. (2023). Encoding normative ethics: On algorithmic bias and disability. First Monday, 28(1). https://doi.org/10.5210/fm.v28i1.12905 (Original work published Jan 16, 2023).
38 Bayton, Douglas. Disability and the Justification of Inequality in American History. Social Welfare History Project, (February 10, 2014). https://socialwelfare.library.vcu.edu/woman-suffrage/disability-justification-inequality-american-history/.
39 Thompson, Vanessa E. "Policing in Europe: Disability Justice and Abolitionist Intersectional Care." Race & Class 62, no. 3 (Jan 1, 2021): 61–76. https://doi.org/10.1177/0306396820966463.
40 Raj, Arushi, and Fatima Juned. "Gendered Identities and Digital Inequalities: An Exploration of the Lived Realities of the Transgender Community in the Indian Digital Welfare State." Gender & Development 30, no. 3 (Sep 2, 2022): 531–49. https://doi.org/10.1080/13552074.2022.2131250.

discuss recommendations for regulation along the lines of "capacity" for responsible use of technologies, rather than the "potentials" of responsible use. We will also consider how structural conditions need to be addressed before implementing technological solutions, and how marginalized communities view bans on biometric technologies.

EXAMINING THE BIOMETRIC BODY

For this report, we interviewed eight key experts:

- Silke Rudolph, Heta Pukki, and Imke Heuer; European Council of Autistic People.
- Dr. Johnathan Flowers, California State University, Northridge.
- Dr. Guy Fagherazzi, Deep Digital Phenotyping Unit, Luxembourg Institute of Health.
- Dr. Beth Semel, Princeton University.
- Dr. Abel Wajnerman Paz, Pontifical Catholic University of Chile.
- Dr. Rafael Yuste, Columbia University.

Additionally, we spoke to Robert Ochshorn, CTO of Reduct.video for technical insights into voice processing technologies.

Technologies that we spotlight include:

- **Voice analytics,** the origins of voice affect in medical studies and the function creep of affect in voice "AI polygraphs."
- **Neurotechnology,** the development of such technologies for medical settings, and the debates around the emerging movement to recognize "neurorights."
- **Eye tracking in VR/AR settings,** the development of eye tracking technologies for medical and educational settings, and the function creep of eye tracking in "AI polygraphs."

We also look at **voice recognition** and **gait analysis**, two types of technologies already deployed in the field, in order to highlight existing privacy and data protection issues.

Within each section of our biometric technology matrix, we look at the existing state of research, questions of explainability, and the future of these technologies, highlighting key reflections from our expert interviews in each section.

THE BIOMETRIC BODY

The Digital Phenotype

HARD BIOMETRICS
N/A

SOFT BIOMETRICS
EEG/ECG for emotional and mental state

HARD BIOMETRICS
Iris scan recognition

SOFT BIOMETRICS
Eye disease (many eye diseases are very noticeable even just from a flash photo)

HARD BIOMETRICS
Face recognition

SOFT BIOMETRICS
BMI (Body Mass Index) detection with face photographs

HARD BIOMETRICS
Voice recognition

SOFT BIOMETRICS
Voice analysis to detect emotional state, disease, and depression via "voice biomarkers"

HARD BIOMETRICS
Breath recognition

SOFT BIOMETRICS
Breath analysis for health (nutrition, alcohol, etc.)

HARD BIOMETRICS
N/A (ECG is not static)

SOFT BIOMETRICS
ECG analysis for heart disease

HARD BIOMETRICS
Unique body odor identification

SOFT BIOMETRICS
Body odor analysis for health

HARD BIOMETRICS
DNA ID

SOFT BIOMETRICS
Genomics and precision medicine (married with EHR)

HARD BIOMETRICS
N/A

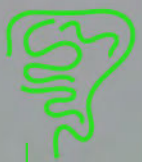
SOFT BIOMETRICS
Blood pressure used for digital health, "lie detectors," and glucose monitoring

HARD BIOMETRICS
Wrist identification (PPG Photo-plethysmography) used often for images of terrorists, actigraphy, and proximity

SOFT BIOMETRICS
Actigraphy is common in Fitbit or other wrist worn health data

HARD BIOMETRICS
Finger print, palm print, palm vein identification

SOFT BIOMETRICS
N/A



HARD BIOMETRICS
N/A (not static)

SOFT BIOMETRICS
Urine and fecal analysis for disease

HARD BIOMETRICS
Gait analysis recognition (not super accurate)

SOFT BIOMETRICS
Gait analysis for physical therapy and disease

Low-tech, soft biometrics

Voice biomarkers

In 2022, as global rates of anxiety, depression, and other mental health illnesses increased by 25 percent[41] from pre-pandemic levels, a small company named Kintsugi filed clinical trial applications to develop technology for detecting anxiety, depression, and mood disorders from what it termed "vocal biomarkers." Based in Berkeley, California, Kintsugi is not a unique byproduct of the Bay Area, but rather part of a growing global, post-pandemic trend of AI-based telehealth apps becoming normalized through large amounts of capital investment.[42] "Digital phenotyping" — the idea that digital products and data could be used for early detection of disease, as well as public health surveillance — is not new, either. Coined by Sachin Jain in 2015, digital phenotyping has also appeared in non-medical contexts such as the quantified self movement (a loose coalition of people and organizations interested in self-health tracking through activity monitors and emerging tech devices).[43] Voice technologies appeared to be a particularly promising direction for telehealth, given the ease of adoption and data capture, the widespread use of mobile phones, and the vast coverage of commercial wireless grids. Capturing voice data can happen with a range of "low-tech" devices, including non-smartphones.[44]

According to researcher Dr. Guy Fagherazzi, the vocal biomarkers field is "booming (...) Everyone is interested [in] collecting voice [data] and trying to find vocal biomarkers, but at the moment it's pretty much the 'far west'; everyone is doing whatever he or she can to develop their own research. And there is no standardization yet." Although research on detecting the presence of neurodegenerative disorders in the human voice began about 30 years ago, the combination of audio signal processing, AI, and deep learning have opened up new opportunities in voice technologies over the past few years.

Dr. Beth Semel explained that a voice "biomarker" is only "mathematically legible in the waveform of a speech (...) a very subtle statistical wrinkle. It doesn't matter what the person is saying, the argument is that vocal biomarkers as an indicator of mental distress are language-agnostic, and expressed by the anatomical fact of producing language."

In a generalized outline of the vocal biomarker development process:[45]

- "Raw" voice data is collected; patients ideally read pre-specified text or use sustained vowel formation (e.g., saying "Ahhhh") for as long as possible. Researchers are increasingly using "free speech" or unstructured audio recording as data.

41 WHO, World Mental Health Report: Transforming mental health for all, (Jun 16, 2022). https://www.who.int/publications-detail-redirect/9789240050860.

42 Williams, Ingrid K., "Can A.I.-Driven Voice Analysis Help Identify Mental Health Disorders?", The New York Times, (Apr 5, 2022). https://www.nytimes.com/2022/04/05/technology/ai-voice-analysis-mental-health.html.

43 Jain, Sachita, Brian W. Powers, Jared B. Hawkins and John S. Brownstein, "The digital phenotype", Nature Biotechnology 33, (May 12, 2105). https://www.nature.com/articles/nbt.3223, and for more on the quantified self movement, see G. Wolf. What is The Quantified Self, (March 2011). https://quantifiedself.com/2011/03/what-is-the-quantified-self/.

44 WHO, mHealth: New horizons for health through mobile technologies, Volume 3. https://www.afro.who.int/publications/mhealth-new-horizons-health-through-mobile-technologie.

45 Thomas JA, Burkhardt HA, Chaudhry S, Ngo AD, Sharma S, Zhang L, Au R, Hosseini Ghomi R. Assessing the Utility of Language and Voice Biomarkers to Predict Cognitive Impairment in the Framingham Heart Study Cognitive Aging Cohort Data. J Alzheimers Dis. 2020;76(3):905-922. doi: 10.3233/JAD-190783. PMID: 32568190., Interview with Dr. Fagherazzi, Singh, Rita. Profiling Humans from Their Voice. 1st ed. 2019. Singapore: Springer Singapore, (2019). Print.

- Audio recordings are processed and transformed to account for background sound and quality, including feature extraction to find key waveform expressions of elements of human speech (e.g., changes in pitch).

- Recordings are fed into machine learning models, training algorithms to predict different health outcomes, symptoms, and diseases.

Recent examples of biomarkers include the detection of COVID-19 via voice recording data, particularly with regards to sounds of coughing and hoarseness.[46] Reproducibility in these research settings has been a significant issue, as we discuss below. Other applications of voice biomarkers include the automated detection of diabetes and dementia via voice.[47] All of these research studies into voice biomarkers, whether in industry or academia, rely on voice as a physiological and psychomotor phenomenon, whereby physical changes or diseases instantiate changes in the voice.[48]

In Rita Singh's often-cited work, "Profiling Humans from Their Voice," voice is cast as a biological acoustic phenomenon based on theories of voice production that border upon the now-discredited fields of phrenology and physiognomy. Sometimes referred to under the umbrella of "race science," humans' physical features were treated in both fields as indicative of intelligence and other cognitive characteristics or capabilities. Singh's work uses size of vocal tract, larynx, age, vocal cord health, and most troublingly, the "race" of a person to make these assessments; e.g. defining "Mongoloid skeletal structures" which create differences in skull types.[49] In contrast to these re-instantiations of phrenology, many other scholars, particularly linguists, have emphasized the ways that pitch, pauses, tone, and emphasis (prosody) in a speaker's "natural" voice are not only socially produced, but also subject to change. For instance, in the face of "linguistic racism," many people adjust and change their voice, implementing "code-switching" practices to be more "neutral"[50] — even as the definition of a "neutral" speaking voice is culturally determined.[51]

Looking to the future, Dr. Fagherazzi believes it may take another five years of clinical trials before such voice biomarker diagnostic tools are commercialized and become subject to approval by regulatory agencies such as the European Medicines Agency (EMA) or the U.S. Federal Drug Administration (FDA). Beyond medical regulatory authorities, regulatory bodies are now looking to govern data use and handling in these biometric systems, as well as

46 Anthes E. Alexa, do I have COVID-19? Nature. (October 2020) ;586(7827):22-25. doi: 10.1038/d41586-020-02732-4. PMID: 32999487. https://pubmed.ncbi.nlm.nih.gov/32999487/.

47 Thomas JA, Burkhardt HA, Chaudhry S, Ngo AD, Sharma S, Zhang L, Au R, Hosseini Ghomi R. Assessing the Utility of Language and Voice Biomarkers to Predict Cognitive Impairment in the Framingham Heart Study Cognitive Aging Cohort Data. J Alzheimers Dis. (2020);76(3):905-922. doi: 10.3233/JAD-190783. PMID: 32568190.

48 Quatieri, T. F. (Thomas F.). Discrete-Time Speech Signal Processing : Principles and Practice. Upper Saddle River, NJ: Prentice Hall, (2002). Print. Singh, Rita. Profiling Humans from Their Voice. 1st ed. 2019. Singapore: Springer Singapore, (2019). Print.

49 ibid. Also see the NeurIPs paper from Rita Singh's lab that attempts to reconstruct facial features using voice, based on these phrenological assumptions. Wen, Yandong, Rita Singh, and Bhiksha Raj. "Reconstructing Faces from Voices." arXiv, (May 31, 2019). https://doi.org/10.48550/arXiv.1905.10604.

50 Chan, Wilfred "The AI startup erasing call center worker accents: is it fighting bias — or perpetuating it?" The Guardian, (Aug 24, 2022). https://www.theguardian.com/technology/2022/aug/23/voice-accent-technology-call-center-white-american and Dovchin, Sender, "Introduction to special issue: linguistic racism", Journal of Bilingual Education and Bilingualism, (May 29, 2020). https://www.tandfonline.com/doi/full/10.1080/13670050.2020.1778630.

51 Aneesh, A. (Aneesh). Neutral Accent : How Language, Labor, and Life Become Global. Durham. Duke University Press, (2015). Print.

examining emerging questions of digital consent. In the U.S., Biometric Information Privacy Acts (BIPA) in several states address the collection of such data, and in the E.U. the GDPR provides individual rights in relation to data collection and processing in biometric systems, which includes protections for voice data.[52] Yet this limited focus on individual rights often fails to address societal- and community-level harms propagated by these technologies, as we will discuss shortly.

Gait analysis

Gait analysis algorithms have been proposed as a form of biometric identification, as well as for use in classification settings — whether to label a person as a potential terrorist "threat," or to classify if someone has a neurodegenerative disease.[53]

Gait is generally defined by how a person walks. Traditionally, visual gait analysis without the help of a computer has been done in biomechanical studies to determine if a person has gait abnormalities; for example, in orthopedic settings or to determine soft tissue or bone abnormalities.[54] Gait data can be collected by cameras or smartphone accelerometers.[55] Given the non-invasive nature of data collection, gait analysis biometric systems could have implications for privacy if data is easily gathered in public places without consent.[56]

Full body motion tracking systems developed for entertainment or video game playing purposes (e.g., computer vision tracking a body to control an avatar) overlaps with development of gait analysis algorithms (computer vision tracking of a body and body segments) — for example, the common use of Microsoft Kinect for playing video games and also markerless body tracking and gait analysis. Gait analysis is an example of biometric systems' potential "function creep."[57]

52 Where voice data would "allow or confirm unique identification" it would be classed as 'biometric data' under the GDPR, and subject to strong protections under Article 9 when used for the purpose of identification. In cases where it was used for profiling or categorisation rather than identification, it would still be classed as personal data and data subjects would retain their rights in relation to it.

53 Priyanka Chaurasia, Pratheepan Yogarajah, Joan Condell, Girijesh Prasad, David McIlhatton & Rachel Monaghan (2015) Biometrics and counter-terrorism: the case of gait recognition, Behavioral Sciences of Terrorism and Political Aggression, 7:3, 210-226, https://doi.org/10.1080/19434472.2015.1071420. Barth, Jens, Jochen Klucken, Patrick Kugler, Thomas Kammerer, Ralph Steidl, Jürgen Winkler, Joachim Hornegger, and Björn Eskofier. "Biometric and Mobile Gait Analysis for Early Diagnosis and Therapy Monitoring in Parkinson's Disease." In the 2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 868–71, (2011). https://doi.org/10.1109/IEMBS.2011.6090226.

54 Skaggs, David L. M.D.; Rethlefsen, Susan A. P.T.; Kay, Robert M. M.D.; Dennis, Sandra W. M.S., P.T.; Reynolds, Richard A. K. M.D.; Tolo, Vernon T. M.D.. Variability in Gait Analysis Interpretation. Journal of Pediatric Orthopaedics 20(6):p 759-764, (November 2000). Saleh M, Murdoch G. In defence of gait analysis. Observation and measurement in gait assessment. J Bone Joint Surg Br. 1985;67-B(2):237-241. doi:10.1302/0301-620X.67B2.3980533

55 Nickel, C., Brandt, H. & Busch, C., (2011). Classification of acceleration data for biometric gait recognition on mobile devices. In: Brömme, A. & Busch, C. (Hrsg.), BIOSIG 2011 – Proceedings of the Biometrics Special Interest Group. Bonn: Gesellschaft für Informatik e.V.. (S. 57-66).

56 Yoo, Jang-Hee, and C.J. Harris. Extracting Human Gait Signatures by Body Segment Properties, (2002). https://doi.org/10.1109/IAI.2002.999885. Boulgouris, N.V., D. Hatzinakos, and K.N. Plataniotis. "Gait Recognition: A Challenging Signal Processing Technology for Biometric Identification." IEEE Signal Processing Magazine 22, no. 6 (November 2005): 78–90. https://doi.org/10.1109/MSP.2005.1550191.

57 Kinect, a popular camera used for the Xbox can be used to perform body tracking as well as gait analysis. M. Gabel, R. Gilad-Bachrach, E. Renshaw and A. Schuster, "Full body gait analysis with Kinect," (2012) Annual International Conference of the IEEE Engineering in Medicine and Biology Society, San Diego, CA, USA, (2012), pp. 1964-1967, https://doi.org/10.1109/EMBC.2012.6346340. Sra, Misha, and Chris Schmandt. "MetaSpace: Full-Body Tracking for Immersive Multiperson Virtual Reality." In Adjunct Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology, 47–48. UIST '15 Adjunct.

Low-tech, hard biometrics

Voice recognition

The processing of vocal outputs in the "vocal biomarker" field, as well as the extraction of statistics from human voice for "diagnostic" capacities, relies on hard biometrics of voiceprint technologies developed within carceral systems. The original "voiceprint" voice recognition technologies were researched and developed by the U.S. National Security Agency (NSA), with the intent to monitor people designated as criminals or of interest to the state during security events.[58] While Apple's Siri and Amazon's Alexa are popular consumer-facing manifestations of voice recognition and voiceprint technologies, Securus, a company that supplies prisons with voiceprint technologies, is funded through a U.S. Department of Defense grant.[59] An example of how such systems are used as "hard" biometrics in prison involves when they purport to identify an inmate making a phone call. Such technologies have increasingly moved in the direction of "soft" biometrics, with claims that software like "Voice IQ" can detect inmates' emotions.[60]

Similar companies are now securing patents for their voiceprint products, funded by military research grants. More troubling than these companies' ties to the military is the reality that without the defense industry and carceral complex, they simply would not exist.[61] A core component of such technologies' political economy is their emergence within markets of carceral and military contractors looking to capitalize on new parts of the population, beyond those designated as "criminal" or "insurgent." Such "function creep" is extremely concerning, given the aforementioned AI reproducibility crisis and the intrinsic inability of machine learning models to generalize predictive capacity with acceptable accuracy across different contexts. For example, a biometric voice system that purports to detect mental distress or anxiety markers may be integrated into "AI lie detectors" deployed by law enforcement or the military.[62] Coupled with flawed science and a lack of reproducibility, deep and irreparable harm is caused when such systems are tasked with making social decisions.

New York, NY, USA: Association for Computing Machinery, (2015). https://doi.org/10.1145/2815585.2817802. Lugrin, Jean-Luc, David Zilch, Daniel Roth, Gary Bente, and Marc Erich Latoschik. "FaceBo: Real-Time Face and Body Tracking for Faithful Avatar Synthesis." In 2016 IEEE Virtual Reality (VR), 225–26, (2016). https://doi.org/10.1109/VR.2016.7504735.

58 Kofman, Ava. "Forget About Siri and Alexa — When It Comes to Voice Identification, the 'NSA Reigns Supreme.'" The Intercept, (Jan 19, 2018). https://theintercept.com/2018/01/19/voice-recognition-technology-nsa/.

59 Nathan, George and Joseph, Debbie. "Prisons Across the U.S. Are Quietly Building Databases of Incarcerated People's Voice Prints." The Intercept, (Jan 30, 2019). https://theintercept.com/2019/01/30/prison-voice-prints-databases-securus/.

60 Lipton, Beryl and Quintin Cooper. "The Catalog of Carceral Surveillance: Voice Recognition and Surveillance." Electronic Frontier Foundation, (Sep 10, 2021). https://www.eff.org/deeplinks/2021/09/catalog-carceral-surveillance-voice-recognition-and-surveillance.

61 Critical Resistance. "What Is the PIC? What Is Abolition?" Critical Resistance, (2022). https://criticalresistance.org/mission-vision/not-so-common-language/.

62 Murphy, Brett. "They Called 911 for Help. Police and Prosecutors Used a New Junk Science to Decide They Were Liars." ProPublica, (Dec 28, 2022). https://www.propublica.org/article/911-call-analysis-fbi-police-courts.
Boguslaw, Daniel. "Lie Detector Firm Lobbies CIA, DOD on Automated Eye-Scanning Tech."
The Intercept, (Apr 7, 2023). https://theintercept.com/2023/04/07/lie-detector-dod-cia-converus/.

High-tech, hard biometrics

Iris scans for ID

The technical development and evolution of iris scans exemplifies how anticipatory governance around biometric technologies is crucial — in particular, the creation of regulatory structures that are willing to outright ban technologies, rather than relying solely on technical expertise around what is considered "public" or "private," intrusive or non-intrusive. In 2005, technical researchers declared iris scans to be "invasive," since data capture needed to happen within close range (e.g., centimeters away). Such a technical constraint meant iris scans were intrusive and would require some form of individual consent around privacy.[63] But by 2010, iris scan technology was refined to a point where data acquisition could happen within meters instead of centimeters, allowing data to be captured about individuals in a more generalized, public setting that drew less attention to how invasive this process remains.[64]

Iris scans are already used in field conditions, and narratives around the use of biometrics in field conditions are particularly interesting. Somaliland, for example, used iris scanning technology in its 2017 elections, reported to be "a high-tech solution that vaults Somaliland ahead of more connected countries such as Nigeria and Kenya.[65] Upon closer inspection, Somaliland did not use biometrics for real-time identification during the polling process, but rather for deduplication of voter registrations, to account for the high-stakes scenario and to prevent real-time biometric failures.[66] Researchers who worked on the voter deduplication system noted that the iris scanning process produces errors, and is affected by eye diseases and the use of contact lenses.[67]

In Jordan, the UNHCR and the World Bank Group's International Finance Corporation have deployed Jordanian-built IrisGuard technology in refugee camps, as well as for the financial inclusion of Syrian migrants.[68] Access to basic needs is then predicated on enrolling in these biometric systems. As Access Now has argued, forcing people with little recourse, such as refugees, to surrender private information in exchange for food is "an affront to human rights standards, and an insult to human dignity."[69] In addition to the opaque government procurement selection process for the company that won the contract, through which Jordan acquired IrisGuard technology, technical assessments of iris scanning systems have shown that such

63 Boulgouris, N.V., D. Hatzinakos, and K.N. Plataniotis. "Gait Recognition: A Challenging Signal Processing Technology for Biometric Identification." IEEE Signal Processing Magazine 22, no. 6 (November 2005): 78–90. https://doi.org/10.1109/MSP.2005.1550191.

64 Ricanek, Karl, Marios Savvides, Damon L. Woodard, and Gerry Dozier. "Unconstrained Biometric Identification: Emerging Technologies." Computer 43, no. 2 (February 2010): 56–62. https://doi.org/10.1109/MC.2010.55.

65 Solomon, Salem, "To Improve Trust in Its Elections, Somaliland Goes High-tech", VOA, (Nov 14, 2017). https://www.voanews.com/a/improve-trust-elections-somaliland-goes-high-tech/4115684.html.

66 Bowyer, Kevin W., Estefan Ortiz, and Amanda Sgroi. Trial Somaliland voting register de-duplication using iris recognition," 2015. 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG), 02:1–8, (2015). https://doi.org/10.1109/FG.2015.7284833.

67 ibid.

68 The UNHCR has used IrisGuard in refugee camps, https://www.accessnow.org/press-release/irisguard-refugees-jordan/ and once outside of refugee camps, the IFC has partnered with IrisGuard for financial inclusion of migrants. https://pressroom.ifc.org/all/pages/PressDetail.aspx?ID=24502.

69 Access Now. Iris scanning of refugees is disproportionate and dangerous — What's happening behind IrisGuard's closed doors? https://www.accessnow.org/press-release/irisguard-refugees-jordan/.

technology, including IrisGuard sensors, produce uneven results depending on the data acquisition environment. This includes variations in lighting, the distance between the eye and the sensor, and pupil dilation at the time of collection.[70]

We cite these examples of iris scanning technology to highlight and underscore the positions of Access Now and other civil society organizations. Despite claims that this technology supports human dignity, it is an affront to basic rights when people are forced to surrender biometric data in order to access basic life-sustaining services, and when vulnerable people's biometric data is used to build and improve biometric systems later sold for profit.[71]

High-tech, soft biometrics

Eye tracking

Similar to voice analytics and neurotech, eye tracking is a research field rife with contradictory claims. Eye tracking refers to tracking of the gaze through "saccades" and "fixations" via the location of the center of the pupil[72] or electrooculography (EOG), which measures changes in the electronic signal around the eyeball. This is then rendered as an "objective" or "scientific" process by means of precise, physiological measurement. Although characteristics about the human eye can be observed and measured, the utility of such measurements for making behavioral assessments is not inherently objective — yet some academic and industry researchers have asserted that eye tracking measurements can be mapped onto attention, emotion, and even diagnoses of disability such as autism, as well as correlations to schizophrenia diagnoses and Alzheimer's disease.[73]

Some researchers note that "in spite of the breadth of existing work, understanding of eye movement pathologies and what they indicate is still limited."[74] Others purport that eye tracking can reveal personality traits, emotional state, and information about a person's ethnic background.[75] As it remains disputed whether a person's identity can be ascertained from simply gaze data itself, there is an open question around whether protections for biometric data, such as those outlined under Article 9 of the GDPR, apply to such data.[76]

70 Connaughton, Ryan, Amanda Sgroi, Kevin Bowyer, and Patrick J. Flynn. "A Multialgorithm Analysis of Three Iris Biometric Sensors." IEEE Transactions on Information Forensics and Security 7, no. 3 (June 2012): 919–31. https://doi.org/10.1109/TIFS.2012.2190575.

71 Zu Nedden, Christina and Dongus, Ariana, "Getestet an Millionen Unfrewilligen," Tested on millions of non-volunteers, translation: https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/01/article_1.pdf, original published in German, Die Zeit, (Dec 17, 2017). https://www.zeit.de/digital/datenschutz/2017-12/biometrie-fluechtlinge-cpams-iris-erkennung-zwang and Osseiran, Nazih, "In Jordan, refugees scan irises to collect aid. But is it ethical?", Reuters, (Dec 13, 2022). https://www.reuters.com/article/jordan-refugees-blockchain/feature-in-jordan-refugees-scan-irises-to-collect-aid-but-is-it-ethical-idUKL8N32R6GF

72 Vidal, Mélodie, et al. "Wearable Eye Tracking for Mental Health Monitoring." Computer Communications, vol. 35, no. 11, (June 2012), pp. 1306–1311, https://doi.org/10.1016/j.comcom.2011.11.002. Duchowski, Andrew. Eye Tracking Methodology: Theory and Practice. Springer Science & Business Media, (Mar 14, 2013).

73 Wan, Guobin, et al. "Applying Eye Tracking to Identify Autism Spectrum Disorder in Children." Journal of Autism and Developmental Disorders, vol. 49, no. 1, (Aug 10, 2018), pp. 209–215, https://doi.org/10.1007/s10803-018-3690-y. And Shic, Frederick, et al. "The Autism Biomarkers Consortium for Clinical Trials: Evaluation of a Battery of Candidate Eye-Tracking Biomarkers for Use in Autism Clinical Trials." Molecular Autism, vol. 13, no. 1, (Mar 21, 2022). https://doi.org/10.1186/s13229-021-00482-2.

74 See supra note 72.

75 Kröger, Jacob Leon, et al. "What Does Your Gaze Reveal about You? On the Privacy Implications of Eye Tracking." Privacy and Identity Management. Data for Better Living: AI and Privacy, (2020), pp. 226–241, https://doi.org/10.1007/978-3-030-42504-3_15.

76 Gressel, Céline, et al. "Privacy-Aware Eye Tracking: Challenges and Future Directions." IEEE Pervasive Computing, vol. 22,

With technical advances in AI data processing, eye tracking equipment is becoming increasingly common. While Pupil Labs (Berlin) offers specialized eye-tracking goggles, new eye-tracking software can now come installed on regular smartphones.[77] In workplace, education, and medical settings, eye tracking and virtual or augmented reality (VR/AR) in particular are seen to be potentially valid automated assessment tools around questions of attention, skills assessment, and job training; e.g. to evaluate surgical skills.[78]

Finally, eye tracking in VR/AR settings can be used for certain functionalities, like advertising or for claims around gauging attention in automobile drivers.[79] Gaze data has been used regularly in "user testing" scenarios, to gauge where users are looking on a webpage or app, and increasingly within apps to allegedly gauge attention to advertisements.[80] Eye tracking, along with face and full body tracking, has also been used to control virtual avatars for entertainment or gaming, or in the case of "aliveness" detection, in biometric systems. A concern in these seemingly benign advertising or entertainment use cases is how such algorithms can be deployed in other contexts — particularly around gait analysis — or for other forms of surveillance, tracking, and profiling.

The proliferation of eye tracking is worrisome for a number of reasons. Despite the regulatory gray area eye tracking operates in as a type of personal, biometric data, and the pseudo-scientific claims around the ability to detect emotion and attention from gaze data, eye tracking is already commercially available, with little regulation around its use. When it comes to diagnostic usage, claims around being able to "diagnose" autism from eye tracking demand careful attention, given the complexity and the ways diagnosis is shaped by care providers' cultural and social contexts — from under-diagnosis of autism in minoritized groups in one country, to the ways social communication vary by cultures.[81] As a representative from the European Council for Autistic People (EUCAP) stated, "[Diagnosis] is something which can't be separated from culture [and] also can't be separated from the individual approach of the person diagnosing, because (...) that will also differ even within a culture. I think you can't get rid of that with autism."

no. 1, (Jan 1, 2023), pp. 95–102, https://doi.org/10.1109/mprv.2022.3228660.

77 Krafka, Kyle, et al. "Eye Tracking for Everyone." The Computer Vision Foundation, (2016).

78 Tien, Tony, and Philip Pucher. "Eye Tracking for Skills Assessment and Training: A Systematic Review." Journal of Surgical Research, vol. 191, no. 1, (Sept 1, 2014), pp. 169–178, www.sciencedirect.com/science/article/abs/pii/S0022480414004326, https://doi.org/10.1016/j.jss.2014.04.032. Duchowski, Andrew T., et al. "Binocular Eye Tracking in vr for Visual Inspection Training." Proceedings of the ACM Symposium on Virtual Reality Software and Technology - VRST '01, (2001). https://doi.org/10.1145/505008.505010.

79 Of note is that the technology for gauging "attention" in drivers is still emergent and there are difficulties around reconciling gaze direction, attention and where drivers are fixated on in their field of vision. Ahlström, Christer, Katja Kircher, Marcus Nyström, and Benjamin Wolfe. "Eye Tracking in Driver Attention Research—How Gaze Data Interpretations Influence What We Learn." Frontiers in Neuroergonomics 2 (2021). https://www.frontiersin.org/articles/10.3389/fnrgo.2021.778043.

80 Schall, Andrew, and Jennifer Romano Bergstrom. "1 - Introduction to Eye Tracking." ScienceDirect, Morgan Kaufmann, (Jan 1, 2014). https://www.sciencedirect.com/science/article/abs/pii/B9780124081383000017. Manfredini, Chiara. "TikTok's "Focused View": A Creepy New Feature." Access Now, (Feb 1, 2023). www.accessnow.org/tiktoks-focused-view-creepy-feature-monetise-your-emotions-2/.

81 Matson, Johnny L. et al. "A Multinational Study Examining the Cross Cultural Differences in Reported Symptoms of Autism Spectrum Disorders: Israel, South Korea, the United Kingdom, and the United States of America." Research in autism spectrum disorders 5.4 (2011): 1598–1604., Begeer, S et al. "Underdiagnosis and Referral Bias of Autism in Ethnic Minorities." Journal of Autism and Developmental Disorders 39.1 (2009): 142–148., Golson, Megan E. et al. "Cultural Differences in Social Communication and Interaction: A Gap in Autism Research." Autism research 15.2 (2022): 208–214.

Neurotech

Broadly conceived, neurotechnology can be categorized as implantable/invasive (embedded within the body) or non-implantable/non-invasive (e.g., wearable headsets) devices that collect and evaluate data on brain activity. As with other examples shared in this paper, machine learning (ML) is used to process and make assessments about data on brain activity (neural data), despite many researchers' inability to fully explain the mechanisms behind certain brain activity from which ML models are identifying patterns. The form that neurotech can take ranges from deep brain stimulators, to neural dust, to wearables,[82] with applications ranging from medical uses through to commercial applications such as gaming. Within this report, we label neurotech as "high-tech," given the advanced level of specialized expertise and medical-grade approvals required to produce and, in some cases, surgically implant the technology. We also categorize it as a type of "soft" biometrics for its uses that capture and make judgments on behavioral attributes.

As with eye-tracking and other biometric systems, military support for neurotech is a core part of how research and development of this technology has been funded. The defense industry is also a site of proposed uses, and a driver of the emerging perception that a global advantage in neurotech could contribute to U.S. military and economic supremacy. Programs such as the U.S. BRAIN Initiative[83] and DARPA N3[84] demonstrate how military interest in neurotech leads to the creation of defense-oriented hubs where academic researchers, industry actors, and other stakeholders convene and develop shared visions for the future of neurotech.

Many of the fears current researchers hold about the future of neurotech involve extrapolations about what present-day advances herald for the not-too-distant future. In an interview for this report, Dr. Rafael Yuste, a leading figure in the "neuro rights" movement, cited studies in which researchers have been able to decode speech[85] and attempts at handwriting[86] in people with impaired speaking and movement as indications of the capabilities that machine learning methods such as neural networks have made possible — far earlier than researchers originally projected. Likewise, he raised the example of research using technology for brain stimulation to enhance memory in older people as a potential site of future inequality between people who have access to memory enhancement and those who do not.[87]

Concerns about the ability both to "read" neural data and to "write" data to the brain have sparked the development of the neuro rights movement as a preemptive response to the future growth of the market for both invasive and non-invasive neurotechnology.

82 Market Analysis: Neurotechnology. Neurorights Foundation, (2023). https://www.canva.com/design/DAFKWDyTHH0/h5RgsTiQ35zWCh2IiiebSA/view.

83 The U.S. BRAIN Initiative. https://braininitiative.nih.gov/.

84 "The Next-Generation Nonsurgical Neurotechnology (N3) program aims to develop high-performance, bi-directional brain-machine interfaces for able-bodied service members. Such interfaces would be enabling technology for diverse national security applications such as control of unmanned aerial vehicles and active cyber defense systems or teaming with computer systems to successfully multitask during complex military missions." Dr. Gopal Sarma. "Next-Generation Nonsurgical Neurotechnology." Defense Advanced Research Projects Agency (DARPA). https://www.darpa.mil/program/next-generation-nonsurgical-neurotechnology.

85 Decoding Speech from Intracortical Multielectrode Arrays in Dorsal "Arm/Hand Areas" of Human Motor Cortex. https://ieeexplore.ieee.org/document/8512199.

86 Willett, Francis R., et al. "High-Performance Brain-To-Text Communication via Handwriting." Nature, vol. 593, no. 7858, (May 1, 2021), pp. 249–254, https://doi.org/10.1038/s41586-021-03506-2.

87 Grover, Shrey, et al. "Long-Lasting, Dissociable Improvements in Working Memory and Long-Term Memory in Older Adults with Repetitive Neuromodulation." Nature Neuroscience, vol. 25, no. 9, (Aug 22, 2022), pp. 1237–1246, https://doi.org/10.1038/s41593-022-01132-3.

WHAT ARE NEURO RIGHTS?

In 2017, a collective of neuroscience and AI researchers, along with representatives from neurotech firms, published an article in Nature laying the foundations for what would later become a core set of "neuro rights:" rights they argued should be championed at an international level to prevent the worst possible outcomes from neurotech's widespread adoption. The five neuro rights of **identity, free will, mental privacy, augmentation, and protection from algorithmic bias** draw inspiration from existing human rights and medical regulations.[88] Yet they seek to raise the stakes of non-adherence early enough that firms are disincentivized from violating these principles. In Dr. Yuste's estimation, efforts to persuade eight major international human rights treaties to incorporate and uphold neuro rights globally will have "more teeth. It's not a soft law, like a lot of the recommendations that are thrown around for AI."

States such as Spain[89] and Brazil[90] have proposed neuro rights-inspired policies for protecting neural data. Chile is the only country in the world to have already enacted neuro rights within its constitution.[91] However, these are not the locations where the fastest-growing commercial activity around neurotech applications are unfolding. Neuro rights proponents hope that achieving international recognition for these five rights would force compliance in countries such as the U.S., where no such bills are under consideration despite having a higher concentration of government and industry funding into neurotech.

88 The NeuroRights Initiative, The Five Neurorights. https://neurorights-initiative.site.drupaldisttest.cc.columbia.edu/sites/default/files/content/The%20Five%20Ethical%20NeuroRights%20updated%20pdf_0.pdf.
89 "'This is not science fiction,' say scientists pushing for 'neuro-rights'." Avi Ascher-Shapiro. Reuters, (Dec 3, 2020). https://www.reuters.com/article/us-global-tech-rights/this-is-not-science-fiction-say-scientists-pushing-for-neuro-rights-idUSKBN28D3HK.
90 "Mind the Gap: Lessons Learned from Neurorights." Karen S. Rommelfanger, Amanda Pustilnik, and Arleen Salles. Science & Diplomacy, (Feb 28, 2022). https://www.sciencediplomacy.org/article/2022/mind-gap-lessons-learned-neurorights.
91 "Worldwide Campaign for Neurorights Notches Its First Win." Eliza Strickland. IEEE Spectrum, (Dec 18, 2021). https://spectrum.ieee.org/neurotech-neurorights.

Within the neuro rights framework, the right to identity involves both informing people about the ways that the use of neurotech may alter their feeling of personal identity, and developing safeguards to ensure that people can retain a sense of self when using these technologies. Free will comprises the ability to make decisions for oneself without being influenced by neurotech inputs, while mental privacy involves regulating the sale and use of neural data. The neuro rights movement's framing of the right to augmentation concerns equal access to the use of neurotech to enhance mental capabilities. And finally, protection from algorithmic bias refers to the inclusion of historically marginalized groups in the process of designing neurotech, to mitigate potential future biased outcomes from these technologies.

CRITICISM OF THE NEURO RIGHTS MOVEMENT

An overarching critique of neuro rights from Latin American digital rights activists is that they are unnecessary, given existing human rights and legal protections. In a critical assessment of Chile's constitutional amendment, Chilean legal scholars argue that neurorights belong to a "'Cartesian reductionist' philosophical thesis, which advocates the need to create new rights in order to shield a specific part of the human body: the brain. Such legislation would obviously be redundant, as the integrity of the whole human being is already safeguarded by the long-standing rights to privacy and to mental and physical integrity."[92] Another argument made by researchers at Derechos Digitales, a Latin America-based digital rights nonprofit, finds neurorights to be an unhelpful framing for the opposite reason: that existing rights to data privacy are ill-protected in Latin America, and that the re-fashioning of pre-existing rights specifically to address one new set of technologies risks constant distraction from ensuring that these rights are protected across as many technologies as possible.[93]

Additionally, neurotech regulation can diminish preexisting legal protections. The text included in the Chilean constitution weakened the absolute guarantee to the "right to life and physical and mental integrity" by incorporating two exceptions: consent and the law. From additional Access Now work with Latin American digital rights groups, there has been wider discomfort with how Spanish-speaking states like Chile and Spain are leading the charge for neuro rights in Latin America–a form of importation of ideas and regulations that do not fit local needs, which some critics characterize as an echo of post-colonial dynamics in the region.

Aside from this far-ranging skepticism of the neuro rights movement, there are also criticisms that take issue with several of the specific proposed rights. One ongoing debate around proposals to regulate neural data hinges on whether to regard these data as analogous to

92 Zúñiga-Fajuri, Alejandra, et al. "Chapter Seven - Neurorights in Chile: Between Neuroscience and Legal Science." ScienceDirect, Academic Press, (Jan 1, 2021). https://www.sciencedirect.com/science/article/abs/pii/S2589295921000059.
93 Garay, Vladmir, et al. "Neuroderechos Para Qué, Maldita Sea." Derechos Digitales, (Apr 29, 2021). https://www.derechosdigitales.org/15760/neuroderechos-para-que-maldita-sea/.

tissues and organs, or to simply classify them as "sensitive data." Internationally, tissues and organs are prohibited from sale or purchase. Therefore, to categorize neural data as requiring a similar level of control would make it next to impossible for neurotech companies to develop applications and hardware trained on neural data.

This raises at least two points of tension. One is that tech firms producing brain-computer interfaces (BCIs) and other neurotech are likely to oppose such a stringent level of proposed regulation. Yet these same firms participate in the community shaping of and advocating for neuro rights. Tech companies are also influential stakeholders in the nascent move to create technical standards for neurotech.[94] It remains to be seen how their commercial interests will square with the proposed neuro right of mental privacy. Some elements of this conflict between regulating neural data akin to organ data, versus regulating neural data as merely "sensitive" data, have already played out in Chile (where neuro rights are enshrined in the constitution) and Brazil (where a proposed neuro rights bill could prohibit data controllers from commercializing neural data).

The second tension involves the nature of what constitutes neural data and, by extension, what it means for an individual to have informed consent in the process of deciding how their data should be used. In an interview for this report, neuroethicist Dr. Abel Wajnerman Paz cautioned that neural data "in some experimental settings or some kinds of applications, may bypass behavior (...) you can profile a person by directly analyzing neural activity, or mental processes." He noted that unlike the ability to control one's behavior, "we don't have control over thoughts and feelings," and therefore current methods of placing the burden back onto the user via informed consent to decide whether or not to opt out are insufficient.

Another ongoing debate concerns whether neuro rights support, or are at odds with, disability rights. As Dr. Wajnerman Paz explains, Chile's experience of regulating consent in research is instructive in thinking about how neuro rights may conflict with other rights. Originally the country had laws that barred conducting research on human subjects who could not give consent, which Dr. Wajnerman Paz noted "completely undermined research related to, for instance, people with disorders of consciousness." He highlighted, however, that within the last two years these laws have changed. In his perspective, a difference emerges here between negative rights (restraining actions against a particular group) and positive rights or capabilities (e.g., claims for a particular group to have access to a resource).

Professor of medical ethics Joseph Fins has argued that there is an imbalance between negative and positive rights within the neuro rights amendment to the Chilean constitution that could hamper research into and development of neurotech assisting with the prognosis, diagnosis, and therapeutics for disorders of consciousness.[95] He characterizes the current framing of neuro rights as being in part predicated on "science fiction"-inspired fears of the

94 IEEE, Standards Roadmap: Neurotechnologies for Brain-Machine Interfacing. IEEE (2020). https://standards.ieee.org/wp-content/uploads/import/documents/presentations/ieee-neurotech-for-bmi-standards-roadmap.pdf.
95 Fins, Joseph J. "The Unintended Consequences of Chile's Neurorights Constitutional Reform: Moving beyond Negative Rights to Capabilities." Neuroethics, vol. 15, no. 3, (Aug 24, 2022). https://doi.org/10.1007/s12152-022-09504-z.

future that could impede present-day scientific advancements, and as being out of step with disability and human rights law. In addition, user-centered design research at a BCI center demonstrated the value of conducting in-person research with disabled people who use these devices, as well as incorporating the tech experiences of these individuals' caregivers into considerations of who constitutes the "end user."[96] Yet it is unclear to what extent these ideas, researched five years ago, have been taken up in neurotech firms to date, or how neuro rights frameworks propose to solicit the input of disabled people.

The commercialization of neurotech applications has created room for ambiguity, in which, as Dr. Wajnerman Paz stated, "the line between medical and non-medical technology is fluid (...) this probably will mean that we will have medical applications that are not regulated by the laws for medical devices." Neurotech has already been incorporated into entertainment and gaming applications, for functions such as controlling gameplay using BCIs rather than physical gaming controllers. Yet as with other examples of function creep in this report, the potential dangerous use of non-invasive neurotech for psychometric evaluations in contexts such as schools or the workplace is not unlikely, given the pathways by which other biometric systems have been folded into these environments.

96 Sullivan, L.S., Klein, E., Brown, T. et al. Keeping Disability in Mind: A Case Study in Implantable Brain–Computer Interface Research. Sci Eng Ethics 24, 479–504 (2018). https://doi.org/10.1007/s11948-017-9928-9.

WHAT ARE THE MAIN ISSUES WITH THE USE OF BIOMETRICS TECHNOLOGIES?

Encouraging an arms race mentality

Aside from burgeoning interest in neurotech that derives from arguments for its potential medical benefits, there has been rising concern, particularly in the U.S., about competition with China on brain-related AI research. This facet of the narrative that the U.S. and China are in an "AI arms race" has spurred a sense of urgency around the need for neurotech research, given U.S. fears of Chinese economic and technological dominance. Publications from U.S. national security-focused researchers assessing the state of Chinese research on brain-inspired AI, connectomics, and BCIs, as well as surveys conducted with Chinese researchers working on these subjects, indicate that the Chinese government has devoted significant resources to making advances in these fields and is outpacing other countries in terms of research funding and publications at major international conferences.[97]

One result of this framing is that many popular media accounts about neurotech echo the same note of urgency around a need for the U.S., and the West in general, to build this technology faster than China.[98] Such accounts both directly and indirectly suggest that if China were to more rapidly develop and adopt neurotech products in everyday life, the rest of the world would be at a disadvantage; from fears that an authoritarian state's dominance in neurotech would be used for both domestic and international surveillance, to worries that the capabilities such technology could grant an entire population would somehow disadvantage other countries.

Despite the speculative and currently unprovable nature of these concerns, they are likely to persist in the public's understanding of neurotech, and therefore also have the potential to influence policymakers. Executives at major tech firms such as Meta have long used the specter of Chinese competition to stave off regulation of their platforms,[99] and similar calls are regularly heard to avoid regulating AI.[100] Civil and human rights advocates should be prepared for this same line of defense to arise around neurotech. In these efforts, it is worth reviewing trends in current Chinese commercialization of BCIs, as well as the noticeable lack of scientific evidence that these applications of neurotech are able to make the kinds of assessments their producers claim.

In 2018, there were reports of companies in China's logistics, energy, and electronic equipment manufacturing sectors requiring

97 Hannas, W. and Chang, H.. "China's "New Generation" AI-Brain Project." National Defense University Press (November 2021). https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2846343/chinas-new-generation-ai-brain-project/, and Hannas, W. Change, H., Aiken C., and Chou, D., China AI-Brain Research, Center for Security and Emerging Technology (September 2020). https://doi.org/10.51593/20190033.

98 Velasquez-Manoff, Moises. "Opinion | the Brain Implants That Could Change Humanity." The New York Times, (Aug 28, 2020). https://www.nytimes.com/2020/08/28/opinion/sunday/brain-machine-artificial-intelligence.html. and Evans, Brad. "Los Angeles Review of Books." Los Angeles Review of Books, (Sep 5, 2022). https://lareviewofbooks.org/article/histories-of-violence-why-we-need-a-universal-declaration-for-neuro-rights/.

99 Toner, Helen, et al. "The Illusion of China's AI Prowess." Foreign Affairs, (Jun 2, 2023). https://www.foreignaffairs.com/china/illusion-chinas-ai-prowess-regulation.

100 Shead, Sam. "U.S. Is "Not Prepared to Defend or Compete in the A.I. Era," Says Expert Group Chaired by Eric Schmidt." CNBC, (Mar 2, 2021). https://www.cnbc.com/2021/03/02/us-not-prepared-to-defend-or-compete-in-ai-era-says-eric-schmidt-group.html.

workers to wear caps that allegedly monitored their brainwaves and transmitted data on their brain activity to management.[101] Without specifying what types of data the caps recorded, journalistic investigations suggested that the devices monitored workers' concentration levels and emotional states. Varying justifications about the use of these caps included claims of improving worker efficiency and ensuring workplace safety, as well as assisting in determining when to grant breaks from work or re-assign a fatigued, distracted, or anxious worker to a less taxing task. Representatives from at least two companies have claimed the use of these caps led to increased profits, yet they did not provide explanations of their methods for making such determinations. Likewise, media reports stated that the use of neurotech in some of these workplaces was "government-backed" without indicating what kinds of support was provided (e.g., subsidies, investment in research and development, requirements that state-owned firms adopt the technology) or which government entities were supplying it, save for the example of NeuroCap, a Ningbo University research project that receives Chinese government funding.

One firm noted it was using the caps in an integration with VR headsets for worker training, wherein the VR headsets would create a simulated workplace training environment. Yet from the descriptions of this combination of VR and neurotech, it was not clear what data the brain activity-monitoring cap would collect or how this would be used. Looking ahead, Chinese researchers have suggested applications in the aviation industry to determine whether pilots are in a suitable emotional state to responsibly fly aircraft. A representative from the firm Deayea claimed that the caps were already being used by high-speed rail train conductors on the heavily-trafficked route between Beijing and Shanghai.

Beyond English-language reporting on Chinese neurotech firms, there is limited public information about similar companies. A notable exception is the Chinese company Huami, which is publicly traded in the U.S. and has partnered with a neuroscience lab at a Chinese university.[102] Huami already provides an ecosystem of wearable health technology, and is thus poised to fold neurotech into this ecosystem in a similar fashion to how emotion recognition capabilities have been appended to edtech software.

Finally, these examples demonstrate how many of the alleged capabilities, proposed uses, and social outcomes of neurotech covered in this report have parallels with non-invasive emotion recognition technologies that do not use neural data as inputs. While this is unsurprising, given that many neurotech applications involve gauging an individual's emotional state, the similarities are worth noting because they warrant similar questioning of whether or not emotions are discrete, measurable characteristics and, if

101 Chen, Stephen. "Chinese Surveillance Programme Mines Data from Workers' Brains." South China Morning Post, (Apr 29, 2018). https://www.scmp.com/news/china/society/article/2143899/forget-facebook-leak-china-mining-data-directly-workers-brains.
102 Advanced Brain Computing Lab, Institute of Advanced Technology University of Science and Technology, China https://iat.ustc.edu.cn/iat/x171/20210312/121.html and Anhui Daily, Huami and School build Brain Computing Lab, http://web.archive.org/web/20230920194301/ , https://www.zhiyuexintong.com/news/information/%E6%A0%A1%E4%BC%81%E5%85%B1%E5%BB%BA%E8%84%91%E6%9C%BA%E6%99%BA%E8%83%BD%E8%81%94%E5%90%88%E5%AE%9E%E9%AA%8C%E5%AE%A4/ and Huami. "Huami Establishes a Brain-Computer Interface Joint Lab with Top Chinese University." PR Newswire, (May 2020). https://www.prnewswire.com/news-releases/huami-establishes-a-brain-computer-interface-joint-lab-with-top-chinese-university-301066695.html.

one believes they are, whether they ought to be captured in the first place.

Lack of reproducibility and explainability

A number of prominent papers and researchers have highlighted the reproducibility crisis particularly within the development of AI models, and the intersection of biological sciences and AI.[103] Many machine learning models are unable to reproduce the results their creators have published, which are deemed as reliable outputs of the models. This reveals how the models' performance runs counter to the extraordinary claims around what AI can actually do.

The lack of reproducibility within AI and machine learning in biometric system settings has been well-documented, even in models already used in clinical settings that collect biometric data to make diagnostic predictions. For example, a sepsis prediction model used by Epic health platform was reproduced by a different researcher and found to be far less accurate than Epic claimed.[104] Other machine learning and AI models, such as flu prediction models, have also been shown to lack reproducibility.[105] A major concern for proprietary or industry-created biometric models is also their opacity; industry does not typically share the data or code necessary for the scientific endeavor of reproducibility. Some scientists have argued that AI and algorithms used in high stakes settings should be subject to an even higher bar of transparency: "If a dataset cannot be shared with the entire scientific community, because of licensing or other insurmountable issues, at a minimum a mechanism should be set so that some highly-trained, independent investigators can access the data and verify the analyses."[106]

The opaque nature of machine learning models can also lead to "data leakage" through what is termed "spurious relationships" between variables in the data: two variables that have no connection to each other producing seeming correlation because of an unseen, third variable.[107] For example, a spurious relationship in vocal biomarkers would occur if the machine learning model yielded a correlation between COVID-19 positive diagnosis and the sound of a train in the voice recording background, but this is due to the hidden, third variable: a COVID-19 voice data collection system being located in a train station. Although the sound of the train in the background has no correlation to COVID infection status, these are the kinds of correlations that can emerge when large amounts of data with an enormous number of dimensions (characteristics) occur.

Other researchers in the field point to the fact that high-profile media hype around irreproducible successes has not induced

103 Narayanan, Arvind. "Reproducibility Workshop." The Reproducibility Crisis in ML-Based Science, Princeton University, (Jul 28, 2022). https://sites.google.com/princeton.edu/rep-workshop.
104 Wong A., Otles E., Donnelly J.P., et al. "External Validation of a Widely Implemented Proprietary Sepsis Prediction Model in Hospitalized Patients." JAMA Internal Medicine 181, no. 8 (Aug 1, 2021): 1065–70. https://doi.org/10.1001/jamainternmed.2021.2626.
105 Nelson N.C., Ichikawa K., Chung J., Malik M.M. "Mapping the Discursive Dimensions of the Reproducibility Crisis: A Mixed Methods Analysis." PLOS ONE 16, no. 7 (Jul 9, 2021): e0254090. https://doi.org/10.1371/journal.pone.0254090.
106 Haibe-Kains, B., Adam, G.A., Hosny, A. et al. Transparency and reproducibility in artificial intelligence. Nature 586, E14–E16 (2020). https://doi.org/10.1038/s41586-020-2766-y.
107 Kapoor, Sayash and Arvind Narayanan. Leakage and the Reproducibility Crisis in ML-based Science, Princeton University (July 2022). https://reproducible.cs.princeton.edu/.

reform of the machine learning field, since some researchers chase hype and media clout outside of academia.[108] Researchers warn that "[t]he research economy cannot turn all its incentives toward novelty, emphasize sensational results to generate attention and prestige outside of academic channels...[f]or digital medicine, it is especially critical to avoid drawing unsubstantiated conclusions from work that appears to rest firmly on impressive gobs of data."[109]

The reproducibility crisis should raise alarm bells for researchers outside the field. Beyond media hype, it is risky and dangerous to bank our well-being on AI models that are far less accurate or reliable than they claim to be. While some argue that "artificial general intelligence" (AGI) will be able to extrapolate across different contexts and that the algorithms themselves will get better, thus alleviating the problem with reproducibility, our interview with Dr. Fagherazzi pointed to the problems with standardized data, with the many ways background noise and different microphones can change data, and with ensuring that the data collected is all of the same quality — i.e., not recordings of people on a train or in a supermarket with background noise. Speaking on the voice biomarker research community, he remarked that:

> "As [in] any AI related research field, we are facing a reproducibility crisis related to AI applications and AI models and also due to the lack of standardized high-quality data... We can definitely have some fairly good performances to detect emotions, feelings, but the lack of reproducibility, again, is the major blocking point to be able to fully trust these technologies. I would like to see the data. I would like to see the results in different settings with different languages with different backgrounds of the population on which you're training the algorithms. This is the type of data and evidence-based results that we are lacking at the moment to be fully trustful of these types of technologies."

Imprecise or low-quality data

The consistency and quality of collected biometric data are integral to reproducibility. When applied in the field, biometric technologies may fail or become unreliable due to inconsistent or low quality data capture.[110] For example, even fingerprint identification systems can fail due to low image quality.[111] Additionally, the data used to train biometric classification algorithms can vary in quality, especially if collected from inconsistent (e.g., non-lab, non-clinical)

108 See supra note 105.

109 Stupple, A., Singerman, D. & Celi, L.A. The reproducibility crisis in the age of digital medicine. npj Digit. Med. 2, 2 (2019). https://doi.org/10.1038/s41746-019-0079-z.

110 W. J. Scheirer, A. Bendale and T. E. Boult. "Predicting biometric facial recognition failure with similarity surfaces and support vector machines," 2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, Anchorage, AK, USA, (2008), pp. 1-8, https://doi.org/10.1109/CVPRW.2008.4563124.

111 E. Tabassi, C.L. Wilson, and C.I. Watson, "Fingerprint Image Quality, NFIQ," in National Institute of Standards and Technology, NISTIR 7151, (2004).

settings. Lighting within images, including iris scans and face tracking can also produce uneven results from biometric algorithms.[112] Failures of biometric systems, which are inevitable as no biometric system is perfect, can produce distrust.[113] As Dr. Fagherazzi summarized, regarding vocal biometric systems, "I think it's very important to move into the realm of clinical trials with standardized processes, where you can really control for audio quality, where you can control for the impact of the age, the gender, the languages, the accents of patients and study participants, because all of this has an impact on the performances."

In addition to data quality issues, there is a gap with all biometric technologies between creating a model for how to measure an object or phenomenon (e.g., emotion), and the chosen methods of obtaining that measurement (e.g., capturing vocal tone, facial muscle movement). As Stark and Hoey[114] have pointed out, the different pairings of models and methods of measuring emotions reveal how "emotion recognition" is itself an imprecise, contestable goal.

The implications of function creep

Function creep, or the expansion of a technology into a use case beyond the original purpose it was developed for, is by now a well-recognized source of ongoing harm in biometric technologies.[115] Researchers have shown that the biometric technology market is highly lucrative, with fierce competition and pressure to constantly patent new technologies — resulting in outsize industry claims around expertise and what technology can do.[116] In tandem with the belief that state investments in technological infrastructure ought to yield maximal value (e.g., the use of CCTV surveillance footage for a wide range of applications beyond policing), these incentives can drive function creep, particularly given claims around veracity and expertise that go unscrutinized.

It is worth restating that biometric technologies in the field are consistently shown to require human interpretation, despite claims that the technology is objective, neutral, or will require no human interpretation.[117] Among our interviewees, some expressed concerns around how technology developed in one setting would, given claims around veracity, be used in another context. For example, a technology that can purportedly detect distress could be used at a border control setting, and cast as a reliable, neutral arbiter of truth.

From a technical research standpoint, some of our interviewees found it troubling to see models with little to no reproducibility being applied across different contexts, and

112 Ricanek, Karl, Marios Savvides, Damon L. Woodard, and Gerry Dozier. "Unconstrained Biometric Identification: Emerging Technologies." Computer 43, no. 2 (February 2010): 56–62. https://doi.org/10.1109/MC.2010.55.
113 Olwig, Karen Fog et al. The Biometric Border World : Technologies, Bodies and Identities on the Move. Ed. Karen Fog Olwig et al. Abingdon, Oxon ;: Routledge, (2020). Print., Bouchiba, Guelta, Redouane Tlemsani, S. Chouraqui, and Mohamed Benouis. "An Improved Behavioral Biometric System Based on Gait and ECG Signals." International Journal of Intelligent Engineering and Systems 12 (Dec 31, 2019): 147–56. https://doi.org/10.22266/ijies2019.1231.14.
114 Luke Stark and Jesse Hoey. (2021). The Ethics of Emotion in Artificial Intelligence Systems. In Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (FAccT '21). Association for Computing Machinery, New York, NY, USA, 782–793. https://doi.org/10.1145/3442188.3445939.
115 Koops, Bert-Jaap. "The Concept of Function Creep." Law, Innovation and Technology 13, no. 1 (Jan 2, 2021): 29–56. https://doi.org/10.1080/17579961.2021.1898299.
116 Olwig, Karen Fog et al. The Biometric Border World : Technologies, Bodies and Identities on the Move. Ed. Karen Fog Olwig et al. Abingdon, Oxon ;: Routledge, (2020). Print.
117 ibid.

deployed in real-world settings via industry claims. This was seen to degrade the standards of peer-reviewed research, and generate broader public distrust around these technologies. This dimension of function creep applies across all quadrants of our biometric technologies matrix; from the use of BCIs for Parkinson's[118] being applied to so-called lie detectors,[119] to the seemingly harmless uses of eye tracking to measure attention in app-based advertising extending to decisions used in law enforcement and border control.

The lack of clarity around the boundaries of what is considered biometric data, as well as what is considered a biometric system, has not only created ambiguous regulations, but also potential for irreversible harm embedded in the market incentives set up for biometric technologies. While biometric identification and biometric data collection are under increased scrutiny by privacy advocates, data sharing for research under the presumed benevolence of public good, for example, the collection of biometric data for curative or diagnostic claims, is overlooked. Of enormous concern is the continued, clear lack of regulation around governance of funding and technological benefits, as well as the adjudication of harms.

In the previously mentioned example where Kintsugi is collecting biometric voice data, conducting clinical trials in partnership with Vituity clinics means that Kintsugi has access to patient health records, populated through centralized Health Information Exchanges that intend to promote interoperability.[120] Within the E.U. the European Commission's proposed European Health Data Space would also allow for industry access to anonymized health data, under the banner of creating innovative health solutions and sparking growth in innovative industries.[121] Scenarios where industry can access health data to create lucrative, for-profit products should be carefully scrutinized by civil society and the public, and policymakers should be prudent in implementation, particularly around questions of data-sharing consent and ways to protect the public. In the U.S. for example, a pharmaceutical company used digital genetic sequence information from cystic fibrosis patients to develop and patent a drug with an annual list price of USD 322,000.[122]

The limits of federated learning

Increasingly popular in the digital health context, federated learning is a machine learning technique "seeking to address the problem of data governance and privacy by training algorithms collaboratively without exchanging the data itself."[123] Across multiple articles and interviews discussing voice biomarkers and neurotech, we saw an increased reliance on technical methods such

118 Sullivan, L.S., Klein, E., Brown, T. et al. Keeping Disability in Mind: A Case Study in Implantable Brain–Computer Interface Research. Sci Eng Ethics 24, 479–504 (2018). https://doi.org/10.1007/s11948-017-9928-9.

119 Świec, J. (2021). Brain-Computer Interface in Lie Detection. In: Paszkiel, S. (eds) Control, Computer Engineering and Neuroscience. ICBCI 2021. Advances in Intelligent Systems and Computing, vol 1362. Springer, Cham. https://doi.org/10.1007/978-3-030-72254-8_17.

120 "Kintsugi Voice Device Study - Full Text View - ClinicalTrials.gov." Clinicaltrials.gov, https://clinicaltrials.gov/study/NCT05554042.

121 European Commission, European Health Data Space Questions and Answers, European Commission - European Commission, https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_2712.

122 Fox, Keolu. "The Illusion of Inclusion — The 'All of Us' Research Program and Indigenous Peoples' DNA." New England Journal of Medicine 383, no. 5 (Jul 30, 2020): 411–13. https://doi.org/10.1056/NEJMp1915987, Nolen, Stephanie and Robbins, Rebecca, "This Drug is a 'Miracle' but These Families Can't Get it", The New York Times, (Feb 9, 2023). https://www.nytimes.com/2023/02/07/health/cystic-fibrosis-drug-trikafta.html.

123 Rieke, Nicola, et al. "The Future of Digital Health with Federated Learning." Npj Digital Medicine, vol. 3, no. 1, (Sep 14, 2020), pp. 1–7, https://www.nature.com/articles/s41746-020-00323-1.

as homomorphic encryption and federated learning for addressing privacy concerns around handling sensitive biometric data.[124]

Yet as Dr. Yuste pointed out, in order to ensure its privacy benefits, "federated learning requires high compliance by the whole field," and at the moment many companies do not use it. Similarly, while Dr. Fagherazzi approves of its use for voice biomarker research, he noted of the field's compliance that "we are not there yet." While federated learning addresses individual privacy concerns, it does not sufficiently address the broader impacts of AI-driven biometric technologies, including the potential for discrimination and highly consequential decision-making predicated on spurious inferences about people. Additionally, while federated learning is an intervention at the technical level with social promises around privacy, a slew of social and technical questions remain around the governance, ownership, and deployment of such models.

Concerns across multiple biometric applications

Among our interviewees who commented on neurotech, some of the biggest concerns raised involved its applications in education and labor contexts. Dr. Yuste noted that he was far more concerned with non-invasive, wearable neurotech because it is more likely to be widely used in the near future, compared to more invasive devices that require neurosurgeons to implant them, and which are thus subject to the scrutiny of medical regulations.

We saw small differences emerge in concerns around how smaller startups, versus bigger or more established tech firms might use neural data. Companies such as Meta have used machine learning for purposes such as inferring the speech that a person is hearing based on that person's neural activity.[125] Business decisions companies make to scale back or completely end work on neurotech can have downstream effects. In 2021, Meta appeared to wind down its work on brain-computer interfaces.[126] There have already been other examples of companies' invasive medical devices, such as retinal implants, being left in patients' bodies with no path to recourse, after the companies who produced them either stopped supporting the product or shuttered altogether.[127] Questions around maintenance of devices if companies go out of business remain largely unanswered in the neurotech field.

Tech companies have also partnered with civil society to produce research on neurotech, such as IBM's work with Future of Privacy Forum.[128] One interviewee expressed concern that tech firms who might want to stave off regulation of neurotech may partner with critics of neuro rights as a way of helping keep companies unaccountable.

124 Ju, Ce, et al. "Federated Transfer Learning for EEG Signal Classification." IEEE Xplore, (Jul 9, 2020). https://ieeexplore.ieee.org/document/9175344. And Wei, Xiaoxi, and A. Aldo Faisal. "Federated Deep Transfer Learning for EEG Decoding Using Multiple BCI Tasks." ArXiv.org, (Feb 6, 2023). https://arxiv.org/abs/2211.10976. Accessed (Sep 20, 2023).
125 King, Jean. "Using AI to Decode Speech from Brain Activity." Ai.facebook.com, (August 2022). https://ai.meta.com/blog/ai-speech-brain-activity/.
126 Regalado, A. "Facebook Is Ditching Plans to Make an Interface That Reads the Brain." MIT Technology Review, (July 2021). https://www.technologyreview.com/2021/07/14/1028447/facebook-brain-reading-interface-stops-funding/.
127 Skerrett, Patrick. "Implant Recipients Shouldn't Be Left in the Dark When a Device Maker Cuts off Support." STAT, (Aug 10, 2022). https://www.statnews.com/2022/08/10/implant-recipients-shouldnt-be-left-in-the-dark-when-device-company-moves-on/stops-funding/.
128 Future of Privacy Forum "Organizations Must Lead with Privacy and Ethics When Researching and Implementing Neurotechnology." (Nov 15, 2021). https://fpf.org/blog/how-neurotechnology-can-benefit-society-while-leading-with-privacy-and-ethics/.

Questions of consent

Some factions of the neurorights community, as well as those who advocate for uses of eye tracking in combination with BCIs for emotion recognition, particularly by disabled or autistic people, argue for notions of "surrogate consent," i.e. that the technology is worth using since it "rehabilitates" people to be able to give consent again.[129]

Yet according to Dr. Johnathan Flowers, ableist social structures provide extremely limited understandings of consent for disabled people: "To folks who would say, 'Well, shouldn't we get them to the level of consent?' I would say, 'Well, shouldn't you better understand how they already are not consenting or what they're consenting to? ...We need to think of the many ways in which people do and do not consent beyond, say, a verbal consent." Examples of non-compliance, resistance, or refusal are all ways that consent is not granted, and can be non-verbal.

Outsourcing social responsibility to technology

Across several interviews, we saw an overall concern that even if biometric systems contain more "diverse" datasets, they can nonetheless reinforce and legitimize harmful ideologies and existing inequities. Dr. Semel expressed how the outsourcing of such technology legitimizes the logic that anyone who has the technology can produce true diagnostics:

> If you're going to take triaging and say, 'It can be done by technology', if you're going to extract it from the expert practitioner, the social worker, the psychiatric nurse, if you're going to say it's possible to, by way of optimizing that decision-making process, say some amount of it – in fact, the most precise part of it – can be outsourced to an AI, you're also opening up the possibility for that expertise to be distributed in a variety of ways to anyone who just has the technology....The parallels there is [are] what really gives me pause with vocal biomarker AI... It's very analogous to... predictive policing or crime-detecting AI. The second that you say, 'It's technically possible to automate pattern recognition work of linking facial features'...to this interior thing called criminal intent, the second that you put that out into the world as a possibility, it's just going to be strategically taken up so that institutions who already do that work of matching externals to internals – aka racism... has a legitimizing function.

These broader concerns have been reflected in specific case studies; for example the ways Frontex border guards become endowed with enormous individual discretion. As Karen Olwig, et al write in their multi-sited study of the European border: "[b]y virtue of the individual discretion they are endowed with, border guards are left with the responsibility for maintaining an acceptable balance between open borders and total closure, as well as between profiling based on

129 Neuroethics: An Ethics of Technology, with Dr. Joseph Fins, Carnegie Council, (Jan 4, 2023). https://www.carnegiecouncil.org/media/series/aiei/neuroethics-ethics-technology-joseph-fins.

appearances and the legally required ethical norms of non-discrimination."[130]

The intermingling of technology with individual discretion becomes evident as border guards navigate larger, organizational, and structural requirements, particularly when the technology that is in use fails. Olwig, et al write:

> [F]or example, Frontex directives require border guards to identify a certain number of so-called high-risk passengers against the guards' perceptions of right and wrong, as well as E.U. laws prohibiting racial profiling. In addition, biometric gates turn into obsolete pieces of machinery disconnected from the border world when they fail to work or are simply switched off by border guards at the airports because the installations "get confused" by the light or by travelers with lots of hand luggage.[131]

In situations like border management, while technology can make claims to function reliably and objectively, failures can place a double burden on border guards to use their personal discretion in decision making and create more uncertainty about whether the technologies actually work.

In non-border contexts, Dr. Semel draws attention to two patterns we see across multiple biometric technologies: the challenge to embodied expertise or clinical knowledge when inscrutable, unaccountable AI methods are applied and repurposed in their stead; and the ways these systems can be quickly repurposed in policing and security contexts to reproduce the very patterns of discrimination that their proponents claim they avoid.

Our EUCAP interviewees echoed this sentiment when it comes to emotion-reading applications of biometrics for autistic people:

> The problems are kind of structural, not in the technology itself, but the way people intend to employ it. There is this massive mistaken assumption that reading emotions in others is somehow central to autism. It isn't. It is a problem that some of us may have. It is not central to autism. And you do not see autistic people anywhere saying, "Please, please create solutions for us to read other people's emotions better." We are saying please develop disability services. Please develop employment. Please develop acceptance. Please give us education, and work, and human dignity. Not please," Devise a gadget for us to tell us that a person is smiling or frowning?"And I've told people that maybe the blind could use that. Somebody went and asked, and they didn't want it either. There is no demand. It is an artificial need created because there's a technology that people desperately want to employ.

130 Olwig, Karen Fog et al. The Biometric Border World : Technologies, Bodies and Identities on the Move. Ed. Karen Fog Olwig et al. Abingdon, Oxon ;: Routledge, (2020). Print.
131 ibid.

Dr. Jonathan Flowers expanded upon this point, noting that:

> When autistic people, people with ADHD or other neurodivergent people, or deaf people, say, "No, I do not want my disability cured. This is a part of who I am. It shapes how I interact with the world and without it, I would be lost," most neurotypical folks are like, "Why would you ever want to remain disabled?" They don't recognize the ways that disabled people are in the world through their bodies and their bodies include their disability.

Finally, our EUCAP respondent surfaced one additional structural pattern, wherein biometric technologies that set a baseline of normative emotional states and behaviors are essentially conditioning all people to perform those states of being. Our respondent characterized these technologies as "sending a message worldwide, to numerous societies and countries, that the ways we express our emotions naturally are wrong, and that we need to be trained to mask them and to perform exactly like other people… that is damaging. That hurts people's mental health. So we don't want the technology being used to encourage that kind of thinking."

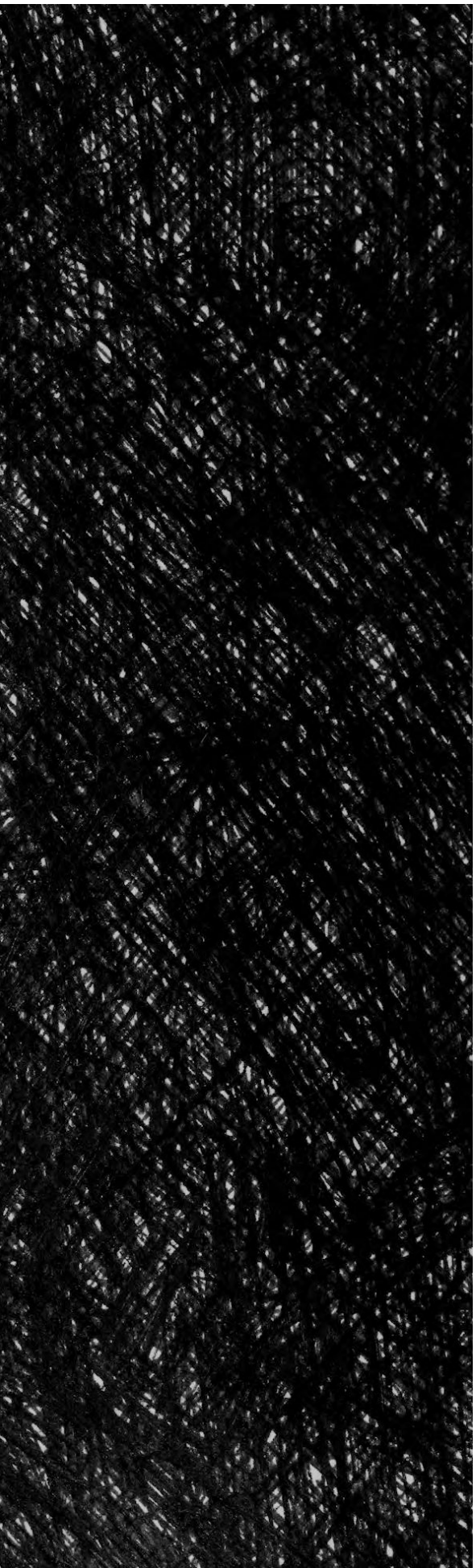
REFLECTING ON REGULATORY GAPS

Throughout the development of the technologies this report covers, as well as the onrush of virtual and extended reality (VR/XR) products that will rely on eye-tracking, BCIs, and other biometrics, the global tech industry operates on the premise that the fundamental issues with biometrics are settled. This report instead argues for advocates to continue unsettling assumptions that biometrics are neutral, fair, and scientifically irreproachable. Before they become taken for granted and embedded in the wave of tech that itself is marketed as remaking "reality," the technologies that we have identified across the matrix of low/high-tech and hard/soft biometrics must be contested and regulated.

Every biometric technology has pre-envisioned a normative, or "correct" idea of a body, and subsequently attempts to fit all bodies that interact with it into this frame. For all of their promise of opening up new possibilities for humans to flourish, what these technologies do instead is the reverse: collapse the varied experiences of human bodies into one single template, and predicate access to resources on whether or not one matches that template.

In an effort to turn this process back on itself as a mode of inquiry, we encourage advocates to note whenever companies and politicians invoke examples of AI and biometric tech as 'curing' disability, and to ask what they are obfuscating or deflecting from in doing so. Most recently, for instance, OpenAI CEO Sam Altman opened his Congressional testimony by describing how the firm's large language model ChatGPT was used by a company called Be My Eyes to describe blind people's surroundings to them through audio. Even though such an example fits our description of assistive, rather than curative, technology, it nonetheless demonstrates how tech representatives invoke and exploit their products' potential value to disabled people as a shield to protect their firms from regulation and public scrutiny.

The expert interviews and literature review conducted for this report gave rise to several insights that may serve civil society advocates seeking to advance regulation and safeguards against the worst harms of biometric systems.



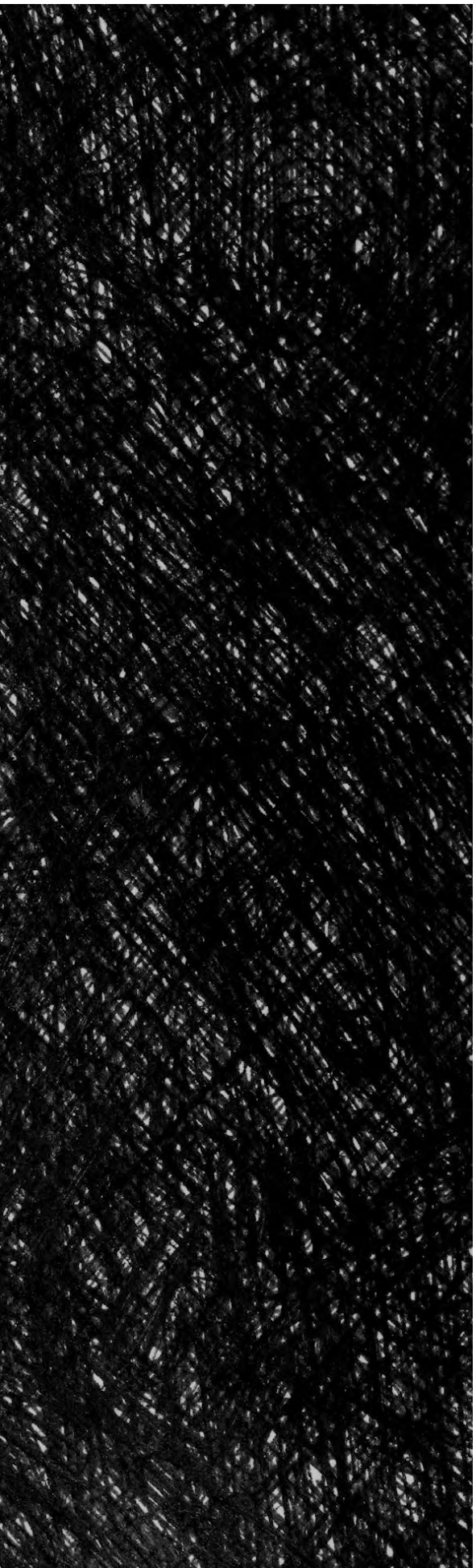
OUR RECOMMENDATIONS

Our first broad recommendation is to identify the distinction between whether a system enacts curative violence (attempting to eradicate a "problem") **or acts as an assistive technology** (attempting to expand an experience or provide feedback that users can act on themselves). In the words of Dr. Flowers:

> A given autistic person might benefit from an autistic burnout app but not want a neural implant that would say, eliminate their autism altogether... It's not simply the right to refuse and right not to have imposed, but the right to choose which biometric or which biomedical technologies are used to expand experience. We need to validate the experiences of all disabled folks and say that there are some disabled folks who simply do not want to be cured and are perfectly okay with the changes in their lives, and there are other disabled persons who will seek biometric methodologies to ameliorate their symptoms. It is a thing that we need to treat experientially and not simply assume that every person with Parkinson's or ALS or any other neurodegenerative disorder wants a cure immediately.

These observations touch upon different approaches to consent beyond individual and group privacy concerns, end-user licensing agreements (EULA), and verbal consent. Starting the research and development of these technologies in consultation with their most marginalized potential users could be a way to surface and design for new conceptions of consent.

Secondly, it's essential to see marginalized groups as builders of technology, not just "users." Researchers and tech companies must go beyond de-biasing to build technologies starting from the viewpoints of those who are most marginalized, and incorporate marginalized communities into governance and decision-making around technology building and making. Policy makers and regulators need to create regulatory pathways that allow for shared governance, benefit, and adjudication of harms in the building, deployment, or banning of certain technologies. It is vital to



incentivize and make explicit the need for companies and organizations building biometric technologies to have stakeholders as active participants in the design and development process. Such regulatory pathways have precedent in the U.S., for instance, where government technology contract tenders include certain requirements in the design and planning process.

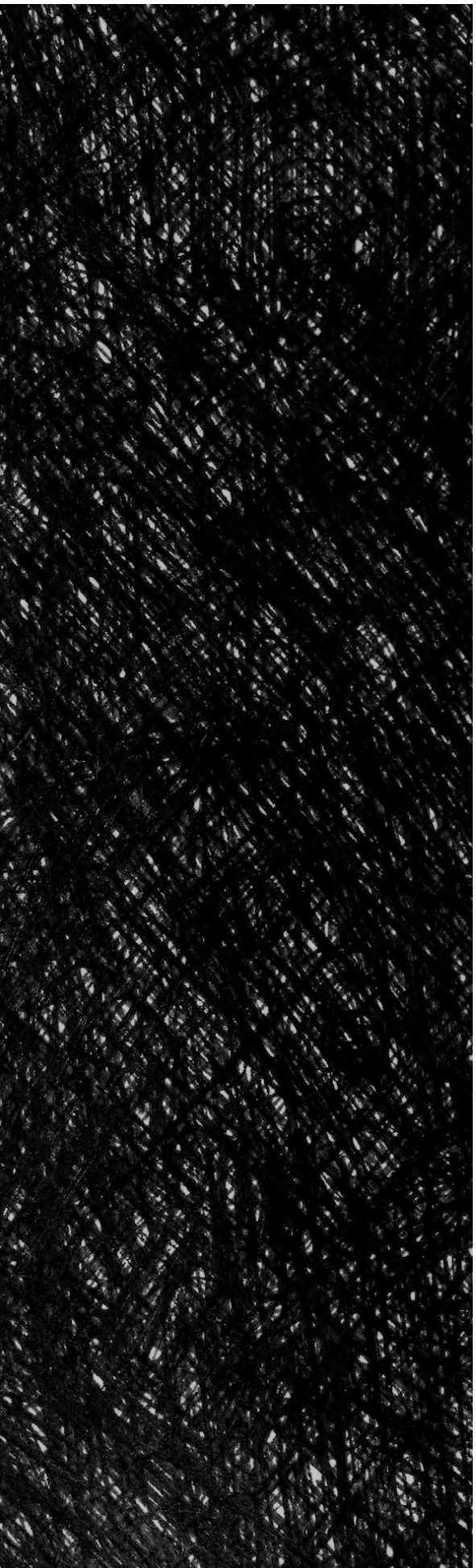
Echoing the sentiments of European Digital Rights' (EDRi) call to move beyond de-biasing AI, we believe it is important to foreground the structural inequities and the context in which biometric systems are deployed,[132] and to think critically about inclusion — inclusion into what system?

For some disability justice advocates, simply being included in technology that perpetuates an ableist system is undesirable. Additionally, including marginalized groups at the last minute in user testing, and using this to claim that the technology built is "un-biased" or "diverse" is inadequate. As we heard from EUCAP: "You can find autistic people who will agree with anything – any individual theory or research question, you will find a few autistic people who will say, 'Yeah, I'm all for it.' But if that is a one in a million person, is it then okay, if the rest of us say, 'No, that's wrong?'"

In Chile, where neuro rights are enshrined in the national constitution, experts we spoke to voiced concerns about the lack of consultation with local communities, placing particular emphasis on the need to hear from disabled people. As Dr. Wajnerman Paz pointed out based on his work with deaf-blind populations in Argentina, in gathering perspectives about how disabled people experience these technologies, there is also a need to solicit the perspectives of their caregivers.

Creating regulatory pathways for shared governance and co-creation of technology that go beyond de-biasing will create more credibility for researchers. To paraphrase Dr. Fagherazzi, "we need transparency [and] co-construction with the patient." In co-creating the technologies, offering shared governance around deployment and benefits can ensure communities will not only feel a more vested stake in these technologies, but greater trust in how these technologies work.

132 Balayn, Agathe and Seda Gürses, Beyond Debiasing: Regulation AI and its inequalities, EDRi, (September 2021). https://edri.org/wp-content/uploads/2021/09/EDRi_Beyond-Debiasing-Report_Online.pdf?ref=salesforce-research.

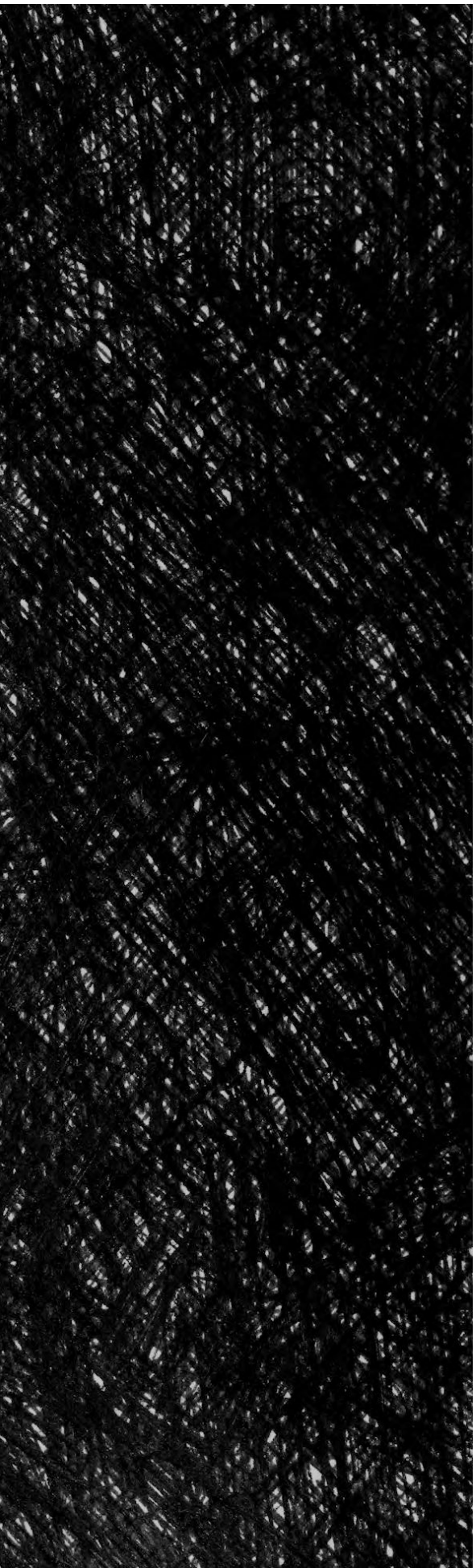


Without these pathways of true co-creation, biometric technologies will create irreconcilable, asymmetrical power dynamics.

Thirdly, we recommend assessing when a biometric technology is used to gate-keep access to benefits and re-entrench asymmetrical power dynamics. Advocates, but also tech companies and regulators, must be aware of the use of biometrics not just within settings that claim to extend experience, but also in settings where biometric technologies are used to gate-keep, contain inequity, or potentially deepen asymmetrical power dynamics between states and communities. This awareness is crucial particularly under fiscal austerity, as states use technologies to replace or augment labor shortages in government services, or to cut costs within state programs — a form of what Dan McQuillan terms "optimizing austerity."[133]

Automation and automated decision-making systems used to determine allocation of social benefits have been shown to create a "digital poorhouse," leaving people trapped in cycles of inequity.[134] Automated systems for fraud detection within social benefits have emerged over the past few years in The Netherlands and Denmark, at times with devastating results. In The Netherlands, false positives impacted tens of thousands of families, leading to unpayable tax bills, children being removed from their families, people losing their homes, and even suicides.[135] As fiscal austerity increases following the COVID-19 pandemic, biometric systems used to diagnose or detect fraud could have harmful, adverse consequences. For example, we heard from EUCAP representatives about the importance of an autism diagnosis in accessing benefits:

133 Tech Won't Save Us, "Why We Must Resist AI W/ Dan McQuillan" Tech Won't Save Us, (Mar 9, 2023). https://techwontsave.us/episode/158_why_we_must_resist_ai_w_dan_mcquillan. Accessed (Sep 20, 2023).
134 Eubanks, Virginia. Automating Inequality : How High-Tech Tools Profile, Police, and Punish the Poor. First edition. New York, NY: St. Martin's Press, (2018). Print.
135 Geiger, G. "How Denmark's Welfare State Became a Surveillance Nightmare." WIRED, (Mar 7, 2023). https://www.wired.com/story/algorithms-welfare-state-politics/, Henley, Jon, and Robert Booth. "Welfare Surveillance System Violates Human Rights, Dutch Court Rules." The Guardian, (Feb 5, 2020). https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules. Heikkilä, Melissa. "Dutch Scandal Serves as a Warning for Europe over Risks of Using Algorithms." POLITICO, (Mar 29, 2022). https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/.



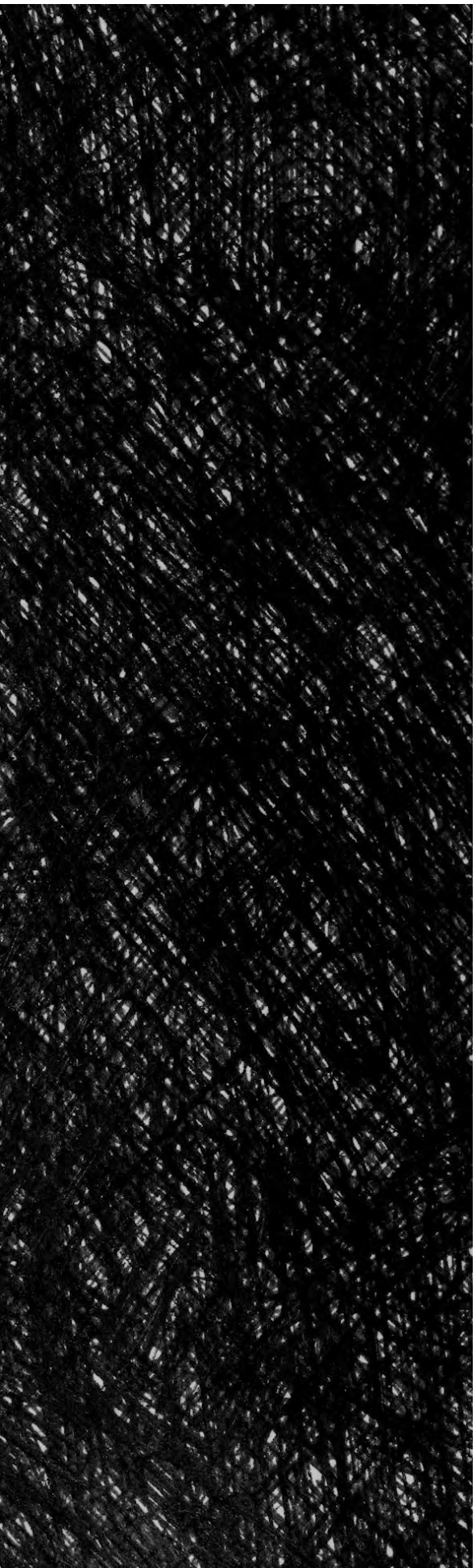
> Diagnosis is complicated, because diagnosis in many parts of the world is the key to services and to being now accepted as having disability status, or adult autism, for example, becoming accepted at all as something that exists...There's all kinds of gatekeeping in Germany, especially for who can give the diagnosis. Is it the psychiatrist [or] a practitioner? Should this be left to university hospitals to do research? And ten or five years ago, they gave a diagnosis to one in three people who went [in] for an assessment. Now it's one in five persons or one in six. So they are getting stricter, and I think it's for economic reasons [supporting people for unemployment]... So I think that's part of the motive unfortunately.

In addressing the use of automation to gate-keep access to state benefits, we can recognize that underneath the question of deploying biometric technologies is a societal question around who we see as "deserving" of state benefits, which often leads to a criminalization of poverty or migrant status.[136]

We also recommend remaining open to bans. While technology bans are often portrayed by the media as an extreme solution, they were raised within the context of our interviews as a way to give some of the most marginalized groups a voice, and as an admission that there are circumstances under which responsible use of a technology may not be possible. Dr. Flowers notes that taking disabled communities' experiences of biometric technologies into account could lead to bans on the technology altogether, explaining that:

> There's a saying that budgets are moral documents...they indicate what a given institution values through the direction of its resources. Regulations are also moral documents insofar as they indicate what a society deems as worth protecting through its legal apparatus...One of the ways we should think about banning is not, Is this technology dangerous, but "Are we capable of using it responsibly?" If the answer is no, then ban the technology.

136 Chunn, D. E., & Gavigan, S. A. M. (2004). Welfare Law, Welfare Fraud, and the Moral Regulation of the 'Never Deserving' Poor. Social & Legal Studies, 13(2), 219-243. https://doi.org/10.1177/0964663904042552.



This reflects a broader, emerging sentiment around how shared decision-making and governance can happen with the building, deploying, and banning of such technologies — where governance is shared beyond the usual stakeholders and industry lobbyists.[137]

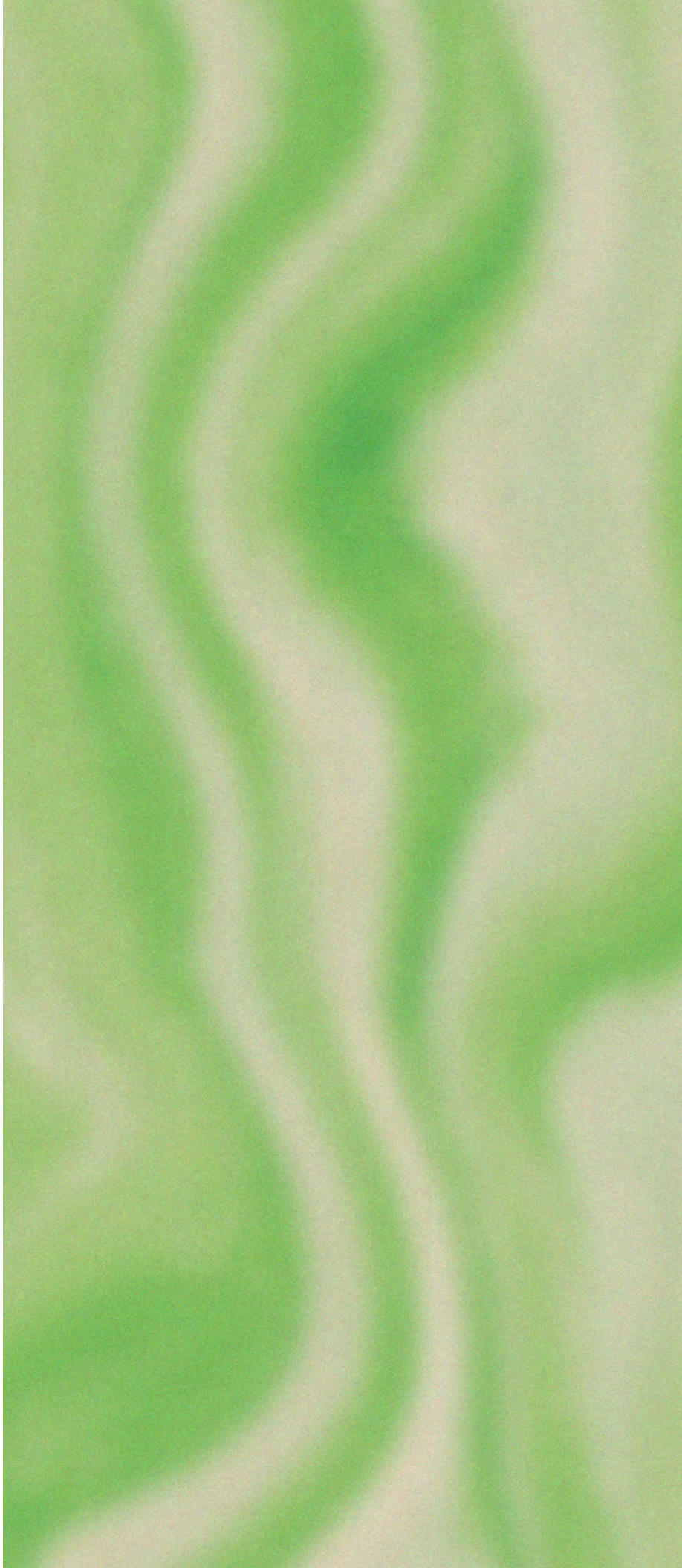
Finally, we recommend cultivating interdisciplinary research spaces and consortia to address structural impacts before a technology is launched. Across our interviews we heard about the need for more interdisciplinarity in the research around all the biometric technologies discussed here. As state-funded consortia such as the National Institutes of Health's Biomarkers Consortium[138] are growing in the U.S. and Europe, they should allocate funding for disability rights scholars, anthropologists, human-computer interaction researchers, and others who study the social and interactive aspects of these technologies, in addition to the funding they provide for medical and technical researchers. Biometric systems do not only include software and algorithms, but also hardware. As many of these biometric technologies rely on research and development of sophisticated hardware devices to collect data, such as the case of BCIs, interdisciplinary consortia and standards setting among researchers creates a salient opportunity for dialogue around ethics, consent, and equity at the early stages of developing such technologies.

If and when tech industry partners participate in these consortia, there should be assurances that their participation is balanced out by the inclusion of researchers from the above-mentioned disciplines, to prevent industry voices from dominating. Finally, we suggest that independent audits of these consortia be conducted to assess for transparency and reproducibility of results, especially those obtained using machine learning.

We opened this report by calling back to the earliest historical forms of biometrics under colonialism, which served as precursors for the advanced technological systems we live with today. Our recommendations work toward a goal of resisting colonization of the future. In other words, we advocate for resistance against the idea that these biometric systems are the inevitable solutions to what are inherently social problems.

137 Solon Barocas, Asia J. Biega, Benjamin Fish, Jędrzej Niklas, and Luke Stark. (2020). When not to design, build, or deploy. In Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT* '20). Association for Computing Machinery, New York, NY, USA, 695. https://doi-org.libproxy.berkeley.edu/10.1145/3351095.3375691.

138 Biomarkers Consortium. Foundation for the National Institutes of Health. https://fnih.org/our-programs/biomarkers-consortium.



accessnow

For more information,
please visit: accessnow.org